Прохоров Ю. Г.

Лекции по алгебре

Семестр 1

Москва 2021

Разъяснение. Настоящие записки появились в процессе подготовки к лекциям. Они нисколько не претендуют на роль учебника.

Оглавление

Лекция 1

Матрицы. Операции сложения и умножения на число. Системы линейных уравнений. Метод Гаусса. Следствия. Системы однородных уравнений.

Матрицы

Матрицей называется таблица

$$C = \begin{pmatrix} c_{1,1} & c_{1,2} & \cdots & c_{1,n} \\ c_{2,1} & c_{2,2} & \cdots & c_{2,n} \\ \cdots & \cdots & \cdots & \cdots \\ c_{m,1} & c_{m,2} & \cdots & c_{m,n} \end{pmatrix}$$

Размером этой матрицы считается $m \times n$ (число строк $\times$ число столбцов). Положение каждого элемента матрицы $c_{i,j}$ задается двумя числами (i, j) (номер строки, номер столбца). Краткая запись матрицы: $C = (c_{i,j})$. Мы рассматриваем также матрицы размера $1 \times n$ (строки) и размера $m \times 1$ (столбцы).

Если λ – произвольное число, то можно определить произведение λ и C:

$$\lambda C = \begin{pmatrix} \lambda c_{1,1} & \lambda c_{1,2} & \cdots & \lambda c_{1,n} \\ \cdots & \cdots & \cdots & \cdots \\ \lambda c_{m,1} & \lambda c_{m,2} & \cdots & \lambda c_{m,n} \end{pmatrix}$$

Если дана еще одна матрица

$$D = \begin{pmatrix} d_{1,1} & d_{1,2} & \cdots & d_{1,n} \\ \cdots & \cdots & \cdots & \cdots \\ d_{m,1} & d_{m,2} & \cdots & d_{m,n} \end{pmatrix}$$

(того же размера), то *сумма* $C + D$ определяется как

$$C + D = \begin{pmatrix} c_{1,1} + d_{1,1} & c_{1,2} + d_{1,2} & \cdots & c_{1,n} + d_{1,n} \\ \cdots & \cdots & \cdots & \cdots \\ c_{1,n} + d_{m,1} & c_{1,n} + d_{m,2} & \cdots & c_{1,n} + d_{m,n} \end{pmatrix}$$

Свойства

. . . . . .

Системы линейных уравнений

Системой линейных уравнений называется система

$$(*) \qquad \begin{cases} a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n &= b_1 \\ a_{2,1}x_1 + a_{2,2}x_2 + \cdots + a_{2,n}x_n &= b_2 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ a_{m,1}x_1 + a_{m,2}x_2 + \cdots + a_{m,n}x_n &= b_m \end{cases}$$

где $a_{i,j}$ и b_i – известные константы, а x_i – неизвестные переменные. Краткая запись этой системы выглядит следующим образом:

$$\begin{cases} \sum_{j=1}^{n} a_{1,j}x_j &= b_1 \\ \sum_{j=1}^{n} a_{2,j}x_j &= b_2 \\ \cdots\cdots\cdots\cdots\cdots \\ \sum_{j=1}^{n} a_{m,j}x_j &= b_m \end{cases}$$

Решением системы называется набор чисел $(c_1, \ldots, c_n)$, которые будучи подставлены в систему $(x_1 = c_1, \ldots, x_n = c_n)$ дают правильные равенства. Система называется *совместной*, если у нее имеется по крайней мере одно решение. Совместная система называется *определенной*, если ее решение единственно.

Система называется *квадратной*, если число ее уравнений равно числу неизвестных $(n = m)$. Система называется *однородной*, если $b_j = 0 \ \forall j$. Отметим, что однородная система обязательно совместна. Говорят, что две системы линейных уравнений от одинакового числа неизвестных *эквивалентны*, если множества их решений совпадают.

Система $(*)$ однозначно задается матрицей

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} & b_1 \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} & b_2 \\ \cdots\cdots & \cdots\cdots & \cdots & \cdots\cdots & \cdots\cdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} & b_m \end{pmatrix}$$

которая называется *расширенной матрицей* системы. Матрица

$$\begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \cdots\cdots & \cdots\cdots & \cdots & \cdots\cdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{pmatrix}$$

называется *матрицей коэффициентов* или просто матрицей системы.

Элементарные преобразования

Определим преобразования $(\mathrm{I}_{\mathrm{i,j},\lambda})$, $(\mathrm{II}_{\mathrm{i},\lambda})$, $(\mathrm{III}_{\mathrm{i,j}})$ $(1 \le i, j \le m$, λ – некоторое число), которые систему $(*)$ переводят в систему

$$(\dagger) \qquad \begin{cases} a'_{1,1}x_1 + a'_{1,2}x_2 + \cdots + a'_{1,n}x_n & = & b'_1 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ a'_{m,1}x_1 + a'_{m,2}x_2 + \cdots + a'_{m,n}x'_n & = & b'_m \end{cases}$$

(I) При преобразовании $(\mathrm{I}_{\mathrm{i,j},\lambda})$ все уравнения $(\dagger)$, кроме i-го имеют тот же вид, а i-е уравнение в $(\dagger)$ принимает вид

$$(a_{i,1} + \lambda a_{j,1})x_1 + (a_{i,2} + \lambda a_{j,2})x_2 + \cdots + (a_{i,n} + \lambda a_{j,n})x_n = b_i + \lambda b_j$$

Иначе говоря, к i-му уравнению прибавляется j-е, умноженное на λ. Здесь считается, что $i \neq j$.

(II) При преобразовании $(\mathrm{II}_{\mathrm{i},\lambda})$ все уравнения $(\dagger)$, кроме i-го имеют тот же вид, а i-е уравнение в $(\dagger)$ принимает вид

$$\lambda a_{i,1}x_1 + \lambda a_{i,2}x_2 + \cdots + \lambda a_{i,n}x_n = \lambda b_i$$

Иначе говоря, к i-е уравнение умножается на λ. Считается, что $\lambda \neq 0$.

(III) При преобразовании $(\mathrm{III}_{\mathrm{i,j}})$ все уравнения $(\dagger)$, кроме i-го и j-го имеют тот же вид, а i-е и j-е уравнения меняются местами. Считается, что $i \neq j$.

Преобразования $(\mathrm{I}_{\mathrm{i,j},\lambda})$, $(\mathrm{II}_{\mathrm{i},\lambda})$, $(\mathrm{III}_{\mathrm{i,j}})$ называются *элементарными преобразованиями* системы.

Замечание. Все элементарные преобразования обратимы. Действительно, обратным к $(\mathrm{I}_{\mathrm{i,j},\lambda})$ является $(\mathrm{I}_{\mathrm{i,j},-\lambda})$, обратным к $(\mathrm{II}_{\mathrm{i},\lambda})$ является $(\mathrm{II}_{\mathrm{i},1/\lambda})$, а обратное преобразование к $(\mathrm{III}_{\mathrm{i,j}})$ совпадает с ним самим.

Замечание. Преобразования типа (III) могут быть получены последовательным применением преобразований типа (I) и (II). Действительно, $(\mathrm{III}_{\mathrm{i,j}})$ получается как композиция $(\mathrm{I}_{\mathrm{i,j},1})$, $(\mathrm{I}_{\mathrm{j,i},-1})$, $(\mathrm{I}_{\mathrm{i,j},1})$ и $(\mathrm{II}_{\mathrm{j},-1})$. (Проверьте!)

Задача. Можно ли преобразования типа (III) получить последовательным применением только преобразований типа (I)?

Предложение. *Если от системы* $(*)$ *можно перейти к системе* $(\dagger)$ *при помощи элементарных преобразований, то эти системы эквивалентны.*

Доказательство. Достаточно доказать наше утверждение для одного преобразования типа (I) или (II). Для (II) утверждение очевидно. Пусть $(\dagger)$ получается из $(*)$ применением одного преобразования типа $(\mathrm{I}_{\mathrm{i,j},\lambda})$. Пусть M (соотв. M') – множество решений

системы $(*)$ (соотв. $(\dagger)$). Если $M = M' = \emptyset$, то доказывать нечего. Поэтому можно считать, что $M \neq \emptyset$. Пусть $(c_1, \ldots, c_n) \in M$. Это означает, что

$$a_{k,1}c_1 + a_{k,2}c_2 + \cdots + a_{k,n}c_n = b_k, \quad \forall k.$$

Так как $a'_{k,l} = a_{k,l}$ и $b'_k = b_k$ при $k \neq i$, то

$$a'_{k,1}c_1 + a'_{k,2}c_2 + \cdots + a'_{k,n}c_n = b'_k, \quad \forall k.$$

Для $k = i$ имеем $a'_{i,l} = a_{i,l} + \lambda a_{j,l}$ и $b'_i = b_i + \lambda b_j$. Отсюда

$$\begin{aligned} a'_{i,1}c_1 + a'_{i,2}c_2 + \cdots + a'_{i,n}c_n &= \\ (a_{i,1} + \lambda a_{j,1})c_1 + \cdots + (a_{i,n} + \lambda a_{j,n})c_n &= \\ a_{i,1}c_1 + \cdots + a_{i,n}c_n + \lambda(a_{j,1}c_1 + \cdots + a_{j,n}c_n) &= \\ b_i + \lambda b_j &= b'_i. \end{aligned}$$

Таким образом, $(c_1, \ldots, c_n) \in M'$ и поэтому $M' \subset M$. Обратное включение следует из обратимости элементарных преобразований. □

Элементарные преобразования матриц

Пусть $A_1, \ldots, A_m$ – строки матрицы A. Мы рассматриваем строки как матрицы и, соответственно, для них определены операции сложения и умножения на число.

Говорят, что матрица A' (того же размера) получена из матрицы A *элементарным преобразованием строк* $(\mathrm{I}_{\mathrm{i,j},\lambda})$, $(\mathrm{II}_{\mathrm{i},\lambda})$, $(\mathrm{III}_{\mathrm{i,j}})$ $(1 \leq i, j \leq m$, λ – некоторое число), если строки $A'_1, \ldots, A'_m$ матрицы A' удовлетворяют следующим условиям:

(I) преобразование $(\mathrm{I}_{\mathrm{i,j},\lambda})$: $A'_i = A_i + \lambda A_j$ и $A'_k = A_k$ при $k \neq i$ (считается, что $i \neq j$);

(II) преобразование $(\mathrm{II}_{\mathrm{i},\lambda})$: $A'_i = \lambda A_i$ и $A'_k = A_k$ при $k \neq i$ (считается, что $\lambda \neq 0$);

(III) преобразование $(\mathrm{III}_{\mathrm{i,j}})$: $A'_i = A_j$, $A'_j = A_i$ и $A'_k = A_k$ при $k \neq i, j$ (считается, что $i \neq j$).

Аналогично можно определить элементарные преобразования *столбцов*.

Определение. Говорят, что матрица

$$C = \begin{pmatrix} c_{1,1} & c_{1,2} & \cdots & c_{1,n} \\ \cdots & \cdots & \cdots & \cdots \\ c_{m,1} & c_{m,2} & \cdots & c_{m,n} \end{pmatrix}$$

имеет *ступенчатый вид*, если она удовлетворяет следующим двум условиям:

(1) Ниже нулевой строки находятся только нулевые строки.

(2) Пусть $1 \leq i < k \leq m$ и пусть $c_{i,j}$ и $c_{k,l}$ – первые ненулевые элементы строк с номером i и k, соответственно. Тогда $l > j$. Иначе говоря, первый ненулевой элемент строки располагается строго правее первого ненулевого элемента любой более верхней строки.

Говорят, что матрица C имеет *улучшенный ступенчатый вид*, если она дополнительно к (1) и (2) удовлетворяет также следующему условию:

(3) Пусть $c_{i,j}$ – первый ненулевой элемент строки с номером i. Тогда $c_{i,j} = 1$ и $c_{r,j} = 0$ для всех r. Иначе говоря, первый ненулевой элемент строки равен 1 и все остальные элементы в столбце, содержащем данный элемент, равны 0.

Метод Гаусса

Теорема (Алгоритм Гаусса). (1) *Любая матрица C элементарными преобразованиями строк типа* (I) *приводится к матрице C', имеющей ступенчатый вид.*

(2) *Любая матрица C элементарными преобразованиями строк типа* (I) *и* (II) *приводится к матрице C', имеющей улучшенный ступенчатый вид.*

Доказательство. Индукция по количеству столбцов n. База индукции $n = 0$ очевидна. Предположим, что наше утверждение верно для всех $n' < n$. Можно считать, что первый столбец $\neq 0$, т.е. $c_{i,1} \neq 0$ для некоторого i. Если $c_{1,1} = 0$, то преобразованием $(\mathrm{I}_{1,i,1})$ добиваемся того, что $c'_{1,1} \neq 0$. Далее, если $c_{i,1} \neq 0$ для некоторого $i > 1$, то преобразованием $(\mathrm{I}_{i,1,\lambda})$, где $\lambda = -c_{i,1}/c_{1,1}$, добиваемся того, что $c'_{i,1} = c_{i,1} + \lambda c_{1,1} = 0$. Таким образом, мы можем считать, что $c_{1,1} \neq 0$ и все элементы в первом столбце кроме $c_{1,1}$ равны 0. Рассмотрим матрицу D, полученную из C вычеркиванием первого столбца и первой строки. По предположению индукции D элементарными преобразованиями строк типа (I) приводится к матрице D', имеющей ступенчатый вид. Проделаем над матрицей C те же элементарные преобразования, что и над матрицей D. Получим матрицу C', в которой все элементы в первом столбце кроме $c'_{1,1}$ равны 0, а матрица, полученная из C' вычеркиванием первого столбца и первой строки, совпадает с D' (и имеет ступенчатый вид). Поэтому и вся матрица C'имеет ступенчатый вид. Это доказывает (1).

(2) Согласно (1) мы можем считать, что матрица C уже имеет ступенчатый вид. Если $c_{i,j}$ – первый ненулевой элемент i-й строки, то преобразованием $(\mathrm{II}_{i,1/c_{i,j}})$ добиваемся того, что $c'_{i,j} = 1$. Далее снова применяем индукцию по числу столбцов. Пусть C_i – последняя ненулевая строка и пусть $c_{i,j} = 1$ – ее первый ненулевой элемент. Тогда $c_{k,j} = 0$ при $k > i$. При $k < i$ преобразованиями $(\mathrm{I}_{k,i,-c_{k,j}})$ добиваемся того, что $c_{k,j} = 0$. Далее используем предположение индукции. □

Определение. Система линейных уравнений называется *ступенчатой*, если таковой является ее расширенная матрица. В этом случае неизвестные, соответствующие столбцам матрицы в которых стоят первые ненулевые элементы строк называются *главными*, а остальные неизвестные – *свободными*. Уравнение вида $0 = b_i$, где $b_i \neq 0$ называется *противоречивым*.

Теорема. *Ступенчатая система совместна тогда и только тогда, когда она не содержит противоречивых уравнений.*

Доказательство. Очевидно, условие необходимо. Докажем его достаточность. Пусть $x_{i_1}, \ldots, x_{i_r}$ – все свободные неизвестные. Придадим им произвольные значения $x_{i_1} =$

$c_{i_1}, \ldots, x_{i_r} = c_{i_r}$ и покажем, что существуют (единственные) значения главных неизвестных, удовлетворяющие нашей ступенчатой системе $(*)$. Действительно, можно считать, что наша система имеет улучшенный ступенчатый вид (при переходе от ступенчатого вида к улучшенному ступенчатому виду свойства неизвестных быть свободными или главными не изменятся). Тогда в каждом нетривиальном уравнении участвует ровно одна главная неизвестная и каждая главная неизвестная участвует ровно в одном нетривиальном уравнении. Таким образом, мы можем выразить главные неизвестные через свободные:

$$x_j = b_i - (a_{i,i_1}x_{i_1} + \cdots + a_{i,i_r}x_{i_r}).$$

□

Следствие. *Для любых значений свободных неизвестных совместной системы существует единственное решение, принимающее эти значения.*

Теорема. *Совместная система определена тогда и только тогда, когда все ее неизвестные – главные.*

Доказательство. Если существует свободная неизвестная, то система не может быть определена по последнему следствию. Если неизвестные – главные, то в улучшенном ступенчатом виде каждое нетривиальное уравнение имеет вид $x_i = b_j$. □

Следствие. *Квадратная система линейных уравнений совместна и определена тогда и только тогда, когда в ее ступенчатом виде нет противоречивых уравнений и соответствующая матрица имеет треугольный вид, т.е.* $a_{i,j} = 0$ *при* $i > j$ *и* $a_{i,i} \neq 0$.

Лекция 2

Умножение матриц. Свойства. Ассоциативность. Матричная запись систем линейных уравнений. Связь однородных и неоднородных систем линейных уравнений. Понятие кольца. Примеры. Умножение на диагональные матрицы. Умножение треугольных матриц. Матричные единицы. Их произведения. Элементарные матрицы. Умножение произвольной матрицы на элементарную. Подстановки. Их произведение. Ассоциативность. Транспозиции. Разложение подстановки в произведение транспозиций.

Умножение матриц.

Пример.

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \qquad \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

Лемма.
- *Пусть A, B, C – матрицы размеров $n \times m$, $n \times m$ и $m \times r$ соответственно. Тогда $(A + B) \cdot C = A \cdot C + B \cdot C$.*
- *Пусть A, B, C – матрицы размеров $n \times m$, $m \times r$ и $m \times r$ соответственно. Тогда $A \cdot (B + C) = A \cdot B + A \cdot C$.*

Доказательство. Пусть $A = (a_{i,j})$, $B = (b_{i,j})$, $C = (c_{i,j})$. Мы можем записать $A + B = (a_{i,j} + b_{i,j})$, $A \cdot C = (d_{i,j})$, $B \cdot C = (f_{i,j})$, $(A + B) \cdot C = g_{i,j}$, где

$$d_{i,j} = \sum_{k=1}^{m} a_{i,k} c_{k,j}, \qquad f_{i,j} = \sum_{k=1}^{m} b_{i,k} c_{k,j}, \qquad g_{i,j} = \sum_{k=1}^{m} (a_{i,k} + b_{i,k}) c_{k,j}.$$

Поэтому $d_{i,j} + f_{i,j} = g_{i,j}$. □

Теорема. *Пусть A, B, C – матрицы размеров $n \times m$, $m \times r$ и $r \times q$ соответственно. Тогда $(A \cdot B) \cdot C = A \cdot (B \cdot C)$.*

Доказательство. Пусть $A = (a_{i,j})$, $B = (b_{i,j})$, $C = (c_{i,j})$. Мы можем записать $A \cdot B = (d_{i,l})$, $B \cdot C = (f_{k,j})$, где

$$d_{i,l} = \sum_{k=1}^{m} a_{i,k} b_{k,l}, \qquad f_{k,j} = \sum_{l=1}^{r} b_{k,l} c_{l,j}.$$

Поэтому $(A\cdot B)\cdot C=(g_{i,j})$, $A\cdot(B\cdot C)=(h_{i,j})$, где

$$g_{i,j}=\sum_{l=1}^{r}d_{i,l}c_{l,j}=\sum_{l=1}^{r}\left(\sum_{k=1}^{m}a_{i,k}b_{k,l}\right)c_{l,j}=\sum_{l=1}^{r}\sum_{k=1}^{m}a_{i,k}b_{k,l}c_{l,j},$$

$$h_{i,j}=\sum_{k=1}^{m}a_{i,k}f_{k,j}=\sum_{k=1}^{m}a_{i,k}\left(\sum_{l=1}^{r}b_{k,l}c_{l,j}\right)=\sum_{k=1}^{m}a_{i,k}\sum_{l=1}^{r}b_{k,l}c_{l,j}.$$

Откуда видно, что $g_{i,j}=h_{i,j}$. □

Замечание. $(A\cdot B)^{\mathrm{T}}=B^{\mathrm{T}}\cdot A^{\mathrm{T}}$. Действительно, пусть $A=(a_{i,k})$, $B=(b_{k,j})$, $A\cdot B=(c_{i,j})$. Тогда $c_{i,j}=\sum_{k=1}^{m}a_{i,k}b_{k,j}$. С другой стороны, положим $A^{\mathrm{T}}=(a'_{j,k})$, $B^{\mathrm{T}}=(b'_{k,i})$, $B^{\mathrm{T}}\cdot A^{\mathrm{T}}=(d_{j,i})$. Тогда $a'_{j,k}=a_{i,k}$, $b'_{k,i}=b_{j,k}$,

$$d_{j,i}=\sum_{k=1}^{m}b'_{k,i}a'_{j,k}=\sum_{k=1}^{m}a_{i,k}b_{k,j}=c_{i,j}.$$

Матричная запись систем линейных уравнений

. . . . . .

Связь однородных и неоднородных систем линейных уравнений.

Для системы линейных уравнений $(*)$ *ассоциированная однородная* система – это система

$$(*)\qquad\begin{cases}a_{1,1}x_1+a_{1,2}x_2+\cdots+a_{1,n}x_n &= 0\\ a_{2,1}x_1+a_{2,2}x_2+\cdots+a_{2,n}x_n &= 0\\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\ a_{m,1}x_1+a_{m,2}x_2+\cdots+a_{m,n}x_n &= 0\end{cases}$$

полученная из $(*)$ занулением свободных членов b_i.

Теорема. *Пусть $(*)$ – любая система линейных уравнений и пусть $(*)$ – ассоциированная с ней однородная система.*

(1) *Если $C=(c_1,\ldots,c_n)$ – решение $(*)$, а $C'=(c'_1,\ldots,c'_n)$ – решение $(*)$, то $C+C'=(c_1+c'_1,\ldots,c_n+c'_n)$ – также решение $(*)$.*

(2) *Если $C=(c_1,\ldots,c_n)$ и $D=(d_1,\ldots,d_n)$ – решения $(*)$, то $C-D=(c_1-d_1,\ldots,c_n-d_n)$ – решение $(*)$.*

(3) *Зафиксируем некоторое решение $C^o=(c^o_1,\ldots,c^o_n)$ системы $(*)$. Тогда любое решение $(*)$ является суммой C^o и некоторого решения $(*)$.*

Теорема. *Рассмотрим систему $AX = B$ линейных уравнений и пусть $X = S'$ – некоторое решение. Тогда любое другое решение $X = S$ представляется в виде $S = S' + L$, где $Y = L$ – решение соответствующей однородной системы $AY = 0$. Обратно, любой столбец вида $S = S' + L$, где $Y = L$ – решение соответствующей однородной системы $AY = 0$ является решением $AX = B$.*

Доказательство. Положим $L := S - S'$. Тогда $AL = AS - AS' = B - B = 0$. Обратно, $AS = AS' + AL = B + 0 = B$. □

Следствие. *Пусть $(*)$ – однородная система линейных уравнений.*

(1) *Если $C = (c_1, \ldots, c_n)$ и $D = (d_1, \ldots, d_n)$ – решения $(*)$, то $+D = (c_1+d_1, \ldots, c_n+d_n)$ – также решение $(*)$.*

(2) *Если $C = (c_1, \ldots, c_n)$ – решение $(*)$, а λ – произвольное число, то $\lambda C = (\lambda c_1, \ldots, \lambda c_n)$ – также решение $(*)$.*

Понятие кольца

Определение. *Кольцом* называется непустое множество R с двумя операциями: сложением $(+)$ и умножением $(\cdot)$ такими, что

(1) (a) $a + (b + c) = (a + b) + c \quad \forall a,\, b,\, c \in R$;

(b) существует элемент $0 \in R$ (нулевой элемент) такой, что $0 + a = a + 0 = a$ $\forall a \in R$;

(c) $\forall a \in R$ существует элемент $-a \in R$ (который называется противоположным к a) такой, что $a + (-a) = (-a) + a = 0$;

(d) $a + b = b + a \quad \forall a,\, b \in R$;

(2) $a \cdot (b + c) = a \cdot b + a \cdot c, \quad (a + b) \cdot c = a \cdot c + b \cdot c \quad \forall a,\, b,\, c \in R$.

Кольцо называется *ассоциативным*, если выполнено свойство

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \qquad \forall a,\, b,\, c \in R.$$

Кольцо называется *коммутативным*, если выполнено свойство

$$a \cdot b = b \cdot a \qquad \forall a,\, b \in R.$$

Единицей кольца называется элемент $1 \in R$ такой, что

$$1 \neq 0 \quad \text{и} \quad 1 \cdot a = a \cdot 1 = a \qquad \forall a \in R.$$

(если такой существует).

Примеры. (1) $\mathbb{Z}$, $n\mathbb{Z}$, $\{a/b \in \mathbb{Q} \mid b \equiv 0 \mod n\}$,

(2) $\mathbb{Q}$, $\mathbb{R}$, $\{a + b\sqrt{2} \in \mathbb{R} \mid a,\, b \in \mathbb{Q}\}$,

(3) $\{a_n\}$ – множество всех последовательностей,

(4) Зафиксируем некоторое множество M. Множество $\{f \mid M \to \mathbb{R}\}$ всех числовых функций на M является кольцом. Множество $C[a,b]$ всех непрерывных функций на отрезке является кольцом.

(5) Множество всех векторов трехмерного пространства с операцией векторного умножения является кольцом.

Теорема. $\mathrm{Mat}_n(\Bbbk)$ – *ассоциативное кольцо с единицей.*

. . . . . .

Матричные единицы.

Матричной единицей назовем матрицу $E_{i,j} = (e_{k,l})$, где

$$e_{k,s} = \begin{cases} 1 & \text{если } k = i \text{ и } l = j, \\ 0 & \text{если } k \neq i \text{ или } l \neq j. \end{cases}$$

Лемма.

$$E_{i,j} \cdot E_{k,l} = \begin{cases} 0 & \textit{если } j \neq k, \\ E_{i,l} & \textit{если } j = k. \end{cases}$$

Элементарные матрицы:

$$U_{i,j,\lambda} = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdot & \lambda & \cdots & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 0 & \cdots & 1 \end{pmatrix}$$

$$U_{i,\lambda} = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & \lambda & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 0 & \cdots & 1 \end{pmatrix}$$

$$U_{i,j} = \begin{pmatrix} 1 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 0 & \cdots & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdot & 1 & \cdots & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 0 & \cdots & 0 & \cdots & 1 \end{pmatrix}$$

Лемма.
- $U_{i,j,\lambda} = E + \lambda E_{i,j}$,
- $U_{i,\lambda} = E + (\lambda - 1)E_{i,i}$,
- $U_{i,j} = E - E_{i,i} - E_{j,j} + E_{i,j} + E_{j,i}$.

Лемма.

$$E_{i,j} \cdot \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \cdots & \cdots & \cdots \\ a_{i,1} & \cdots & a_{i,n} \\ \cdots & \cdots & \cdots \\ a_{n,1} & \cdots & a_{n,n} \end{pmatrix} = \begin{pmatrix} 0 & \cdots & 0 \\ \cdots & \cdots & \cdots \\ a_{j,1} & \cdots & a_{j,n} \\ \cdots & \cdots & \cdots \\ 0 & \cdots & 0 \end{pmatrix}$$

Действительно, пусть $E_{i,j} = (e_{k,l})$ и $E_{i,j}A = C = (c_{k,l})$. Тогда

$$c_{k,l} = \sum_{s=1}^{n} e_{k,s}a_{s,l} = e_{k,j}a_{j,l} = \begin{cases} a_{j,l} & \text{если } k = i, \\ 0 & \text{если } k \neq i. \end{cases}$$

Теорема. *Пусть $A \in \mathrm{Mat}_n(\Bbbk)$, пусть U – одна из элементарных матриц $U_{i,j,\lambda}$, $U_{i,j,\lambda}$, $U_{i,j,\lambda}$. Тогда матрица $U \cdot A$ получается из A соответствующим элементарным преобразованием* $(\mathrm{I}_{\mathrm{i,j},\lambda})$ $(\mathrm{II}_{\mathrm{i},\lambda})$, $(\mathrm{III}_{\mathrm{i,j}})$.

Подстановки

Свойства отображений

Два отображения $f : X \to Y$ и $g : X \to Y$ считаются *равными*, если $f(x) = g(x)$ $\forall x \in X$. *Тождественное* отображение множества X в себя будет обозначаться ε_X или просто ε. Таким образом, $\varepsilon(x) = x$ $\forall x \in X$. Напомним, что *композицией* отображений $f : X \to Y$ и $g : Y \to Z$ называется отображение $g \circ f : X \to Z$ такое, что $g \circ f(x) = g(f(x))$.

Теорема. *Рассмотрим отображения $f : X \to Y$, $g : Y \to Z$ и $h : Z \to U$. Тогда $(h \circ g) \circ f = h \circ (g \circ f)$.*

Доказательство. Для любого $x \in X$ имеем

$$(h \circ g) \circ f(x) = (h \circ g)(f(x)) = h(g(f(x))),$$

$$h \circ (g \circ f)(x) = h((g \circ f)(x)) = h(g(f(x))).$$

Следовательно, $h(g(f(x))) = h(g(f(x)))$. □

Отображение $f : X \to Y$ называется *инъективным*, если из того, что $f(x_1) = f(x_2)$ следует $x_1 = x_2$. Оно называется *сюръективным*, если для любого $y \in Y$ существует $x \in X$ такое, что $f(x) = y$. Отображение $f : X \to Y$ называется *биективным* если оно инъективно и сюръективно.

Пусть дано отображение $f : X \to Y$. *Обратным* к нему называется отображение $f^{-1} : Y \to X$ такое, что $f \circ f^{-1} = \varepsilon_Y$ и $f^{-1} \circ f = \varepsilon_X$.

Предложение. (1) *Обратное отображение к $f : X \to Y$ существует $\iff$ f биективно.*

(2) *Если обратное отображение к $f : X \to Y$ существует, то оно единственно.*

Доказательство. ..... □

Подстановки

Рассмотрим множество $\Omega_n := \{1, \dots, n\}$. Подстановкой называется любое биективное отображение $\sigma : \Omega_n \to \Omega_n$. Множество всех подстановок обозначим через S_n. Каждая подстановка однозначно $\sigma \in S_n$ задается $2 \times n$-таблицей (матрицей)

$$\begin{pmatrix} i_1 & i_2 & \cdots & i_{n-1} & i_n \\ j_1 & j_2 & \cdots & j_{n-1} & j_n \end{pmatrix}$$

где $\{i_1, \dots, i_n\} = \Omega_n$ и $j_k := \sigma(i_k)$. Такая запись не единственна: при перестановке столбцов мы получаем ту же подстановку. Таким образом, каждая подстановка может быть записана в стандартном виде

$$\begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ j_1 & j_2 & \cdots & j_{n-1} & j_n \end{pmatrix}$$

Назовем *перестановкой* из n элементов строку $(i_1, \dots, i_n)$, где $i_k \in \Omega_n$ и $i_k \neq i_l$ при $k \neq l$. Ясно, что для перестановки $(i_1, \dots, i_n)$ всегда выполнено $\{i_1, \dots, i_n\} = \Omega_n$.

Произведением подстановок σ_1, $\sigma_2 \in S_n$ назовем их композицию $\sigma_1 \circ \sigma_2 \in S_n$. Тождественная подстановка обозначается через ε.

Свойства подстановок.

- $(\sigma \circ \varphi) \circ \delta = \sigma \circ (\varphi \circ \delta)$ для всех $\sigma, \varphi, \delta \in S_n$ (ассоциативность);
- $\sigma \circ \varepsilon = \varepsilon \circ \sigma = \sigma$ для всех $\sigma \in S_n$;
- $\forall\ \sigma \in S_n\ \exists\ \sigma^{-1} \in S_n \quad \sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = \varepsilon$.

Определение. *Транспозицией* называется подстановка $\tau \in S_n$ такая, что существуют i, $j \in \{1, \dots, n\}$, $i \neq j$ такие, что $\tau(i) = j$, $\tau(j) = i$ и $\tau(k) = k$ при $k \notin \{i, j\}$. Эта транспозиция обозначается $\sigma = [i, j]$.

Теорема. *Любая подстановка $\sigma \in S_n$ представляется в виде произведения транспозиций: $\sigma = \tau_1 \circ \cdots \circ \tau_r$.*

Доказательство. Индукция по n. Предположим, что утверждение верно для $n - 1$. Пусть

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ i_1 & i_2 & \cdots & i_{n-1} & i_n \end{pmatrix}$$

Если $i_n \neq n$, то рассмотрим транспозицию $\tau = [n, i_n]$. Если же $i_n = n$, то положим $\tau = \varepsilon$. В обоих случаях

$$\tau \circ \sigma = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ i'_1 & i'_2 & \cdots & i'_{n-1} & n \end{pmatrix}$$

Рассмотрим подстановку

$$\sigma' = \begin{pmatrix} 1 & 2 & \cdots & n-1 \\ i'_1 & i'_2 & \cdots & i'_{n-1} \end{pmatrix} \in S_{n-1}$$

По предположению индукции она раскладывается в произведение транспозиций: $\sigma' = \tau'_1 \circ \cdots \tau'_m$, $\tau'_i = [k_i, l_i] \in S_{n-1}$, $k_i\ l_i \in \{1, \ldots, n-1\}$, $k_i \neq l_i$. Рассмотрим транспозиции $\tau_i = [k_i, l_i] \in S_n$. Очевидно, что $\tau \circ \sigma = \tau_1 \circ \cdots \circ \tau_m$. Поэтому $\sigma = \tau \circ \tau_1 \circ \cdots \circ \tau_m$. □

Для перестановки $\Pi = (i_1, \ldots, i_n)$ и подстановки $\sigma \in S_n$ положим $\sigma(\Pi) = (\sigma(i_1), \ldots, \sigma(i_n))$. Ясно, что $\sigma(\Pi)$ – перестановка и $\delta \circ \sigma(\Pi) = \delta(\sigma(\Pi))$.

Следствие. *Любые две перестановки из одинакового числа элементов могут быть получены друг из друга применением конечного числа транспозиций.*

Доказательство. Пусть $\Pi = (i_1, \ldots, i_n)$ и $\Pi' = (j_1, \ldots, j_n)$. Рассмотрим подстановку

$$\sigma = \begin{pmatrix} i_1 & i_2 & \cdots & i_{n-1} & i_n \\ j_1 & j_2 & \cdots & j_{n-1} & j_n \end{pmatrix}$$

По теореме $\sigma = \tau_1 \circ \cdots \circ \tau_r$, где τ_k – транспозиции. Тогда

$$\Pi' = \sigma(\Pi) = \tau_1 \circ \cdots \tau_r(\Pi) = \tau_1(\tau_2(\cdots \tau_r(\Pi)))$$

□

Лекция 3

Запись подстановок. Обратная и единичные подстановки. Понятие группы. Примеры. Число подстановок. Неподвижные элементы. Независимые подстановки коммутируют. Циклы. Разложение подстановки в произведение независимых циклов. Применение подстановки к перестановке. Четность. Корректность определения четности (как меняется число инверсий при применении транспозиции).

. . . . . .

Понятие группы

Определение. *Группой* называется множество G с операцией $(a, b) \mapsto a \circ b$. Такое, что выполняются свойства:

(1) $a \circ (b \circ c) = (a \circ b) \circ c \quad \forall a,\, b,\, c \in G$;

(2) существует элемент $1 \in G$ (единичный элемент или нейтральный элемент) такой, что $1 \circ a = a \circ 1 = a \quad \forall a \in G$;

(3) $\forall a \in G$ существует элемент $a^{-1} \in G$ (который называется обратным к a) такой, что $a \circ a^{-1} = a^{-1} \circ a = 1$.

В определении выше операция $\circ$ "похожа" на операцию умножения. В этом случае говорят, что группа записана *мультипликативно*. Иногда операция в группе записывается *аддитивно*. Тогда определение выше принимает вид:

Определение. Аддитивной группой называется множество G с операцией $(a, b) \mapsto a+b$. Такое, что выполняются свойства:

(1) $a + (b + c) = (a + b) + c \quad \forall a,\, b \in G$;

(2) существует элемент $0 \in G$ (нулевой элемент) такой, что $0 + a = a \circ 0 = a \quad \forall a \in G$;

(3) для любого $a \in G$ существует элемент $-a \in G$ (который называется противоположным к a) такой, что $a + (-a) = (-a) + a = 0$.

В мультипликативной группе имеет смысл понятие целой степени элемента: если $a \in G$ и $n \in \mathbb{Z}$, то

$$a^n = \begin{cases} \underbrace{a \circ \cdots \circ a}_{n} & n \in \mathbb{N}, \\ 1 & n = 0, \\ (a^{-1})^{-n} & -n \in \mathbb{N}. \end{cases}$$

Возведение в степень удовлетворяет стандартным свойствам:

$$a^n \circ a^m = a^{n+m} = a^m \circ a^n, \qquad (a^n)^m = (a^m)^n = a^{nm}.$$

В аддитивной группе понятие степени заменяется на понятием умножения на целые числа: если $a \in G$ и $n \in \mathbb{Z}$, то

$$na = \begin{cases} \underbrace{a + \cdots + a}_{n} & n \in \mathbb{N}, \\ 0 & n = 0, \\ n(-a) & -n \in \mathbb{N}. \end{cases}$$

Определение. Группа G называется *абелевой* (или *коммутативной*), если $a \circ b = b \circ a$ $\forall a, b \in G$.

Обычно группа, записанная аддитивно, предполагается абелевой.

Предложение. *Пусть G – группа. Тогда*

(1) *нейтральный элемент – единственный;*

(2) *для любого $a \in G$ обратный элемент a^{-1} – единственный;*

(3) *для любых $a, b \in G$ уравнение $a \circ x = b$ (соотв. уравнение $x \circ a = b$) имеет единственное решение.*

Примеры. (1) Группа подстановок S_n. Подгруппа четных подстановок $A_n \subset S_n$.

(2) Группа невырожденных матриц $GL_n(\Bbbk)$ над полем $\Bbbk$ (полная линейная группа). Подгруппа $SL_n(\Bbbk) \subset GL_n(\Bbbk)$ матриц с определителем 1 (специальная линейная группа).

(3) $\mathbb{Z}^+$, $\mathbb{Q}^+$, $\mathbb{R}^+$,

(4) $\mathbb{Q}^*$, $\mathbb{R}^*$, $\{\pm 1\}$.

Предложение. *Число число всех подстановок равно числу всех перестановок и равно $n!$.*

. . . . . .

Циклы

Определение. Пусть $\sigma \in S_n$. Элемент $j \in \{1, \dots, n\}$ называется *неподвижным* для σ, если $\sigma(j) = j$ и *подвижным*, если $\sigma(j) \neq j$. Множество всех неподвижных элементов мы обозначим через $F(\sigma)$, а множество всех подвижных – через $M(\sigma)$.

Замечание. Ясно, что $M(\sigma_1 \circ \sigma_2) \subset M(\sigma_1) \cup M(\sigma_2)$ и $F(\sigma_1 \circ \sigma_2) \supset F(\sigma_1) \cap F(\sigma_2) \quad \forall \sigma_1, \sigma_2 \in S_n$.

Лемма. *Если для подстановок $\sigma, \varphi \in S_n$ выполнено $M(\sigma) \cap M(\varphi) = \emptyset$, то $\sigma \circ \varphi = \varphi \circ \sigma$ (т.е. σ и φ коммутируют).*

Определение. Подстановка $\sigma \in S_n$ называется *циклом* (*циклической подстановкой*), если $M(\sigma) = \{i_1, \dots, i_m\}$ и

$$\sigma(i_k) = \begin{cases} i_{k+1} & \text{при } k = 1, \dots, m-1, \\ i_1 & \text{при } k = m. \end{cases}$$

Такая подстановка обозначается $\sigma = [i_1, \dots, i_m]$. Число m называется *длиной* цикла.

Цикл длины 2 – это транспозиция. Запись $\sigma = [i_1, \dots, i_m]$ не единственна. Ясно, что $[i_1, \dots, i_m] = [i_2, \dots, i_m, i_1] = [i_3, \dots, i_m, i_1, i_2]$ и т. д.

Циклы $\sigma = [i_1, \dots, i_m]$ и $\varphi = [j_1, \dots, j_l]$ называются *независимыми*, если $M(\sigma) \cap M(\varphi) = \emptyset$.

Теорема. *Любая подстановка $\sigma \in S_n$ представляется в виде произведения независимых циклов $\sigma = \sigma_1 \circ \cdots \sigma_l$. Это произведение единственно с точностью до порядка множителей.*

Доказательство. Докажем утверждение индукцией по числу элементов в $M(\sigma)$. Пусть $i_1 \in M(\sigma)$ – подвижный элемент. Положим $i_k := \sigma^{k-1}(i_1)$. Таким образом, $i_{k+1} = \sigma(i_k)$. Все элементы $i_1, i_2, \dots \in \Omega_n$ не могут быть различны. Поэтому $i_{k+r} = i_k$ для некоторых $k,\ r \in \mathbb{N}$. Выберем $k,\ r \in \mathbb{N}$ – так, что r – наименьшее, удовлетворяющее этому условию. Тогда для все числа $i_1, \dots, i_r$ различны и

$$i_{r+1} = \sigma^r(i_1) = \sigma^{-(k-1)}(\sigma^{k-1+r}(i_1)) =$$
$$= \sigma^{-(k-1)}(i_{k+r}) = \sigma^{-(k-1)}(i_k) = \sigma^{-(k-1)}(\sigma^{k-1}(i_1)) = i_1.$$

Положим $\sigma_1 := [i_1, \dots, i_r]$ и $\sigma' = \sigma \circ \sigma_1^{-1}$. Имеем

$$\sigma'(i_k) = \begin{cases} \sigma(i_r) = i_1 & \text{при } k = 1, \\ \sigma(i_{k-1}) = i_k & \text{при } k = 2, \dots, r \end{cases}$$

т.е. $i_k \in F(\sigma') \quad k = 1, \dots, r-1$. Если же $j \notin \{i_1, \dots, i_r\}$, то $\sigma'(j) = \sigma(j)$. Таким образом, $M(\sigma) = M(\sigma') \cup M(\sigma_1)$ и $M(\sigma') \cap M(\sigma_1) = \emptyset$. Единственность!

. . . . . .

□

Определение. Рассмотрим перестановку $\Pi = (i_1, \ldots, i_k, \ldots, i_l, \ldots, i_n)$. По определению перестановки $i_k \neq i_l$ при $k \neq l$. Пусть $k < l$. Если $i_k > i_l$, то мы будем говорить, что элементы i_k и i_l образуют инверсию. *Четностью* перестановки назовем четность общего числа инверсий.

Пример. Пусть $1 \leq i < j \leq n$. Число инверсий в перестановке

$$(1, 2, \ldots i-1, j, i+1, \ldots, j-1, i, j+1, \ldots, n-1, n)$$

равно $j - i + \underbrace{1 + \cdots + 1}_{j-i-1} = 2(j-i) - 1$. Поэтому перестановка – нечетная.

Лемма. *Четность перестановки меняется при применении транспозиции.*

Доказательство. Пусть $\Pi = (i_1, \ldots, i_n)$, пусть $\tau = [a, b]$, $a \neq b$. Ясно, что $a = i_k$, $b = i_l$ для некоторых $i_k \neq i_l$, $k < l$. Таким образом, $\Pi = (i_1, \ldots, i_k, \ldots, i_l, \ldots, i_n)$ и $\tau = [i_k, i_l]$. Тогда $\tau(\Pi) = (i_1, \ldots, i_l, \ldots, i_k, \ldots, i_n)$. Обозначим через r_α (соотв. s_α)) число инверсий, которые образует число, стоящее на месте α в Π (соотв. $\tau(\Pi)$) со всеми последующими. Рассмотрим сначала случай $l = k + 1$. Если $\alpha < k$ или $\alpha > k + 1$, то $r_\alpha = s_\alpha$). Для $\alpha = k$ и $\alpha = k + 1$ имеем

$$s_k = \begin{cases} r_{k+1} + 1 & \text{если } i_k < i_{k+1} \\ r_{k+1} & \text{если } i_k > i_{k+1} \end{cases}$$

$$s_{k+1} = \begin{cases} r_k & \text{если } i_k < i_{k+1} \\ r_k - 1 & \text{если } i_k > i_{k+1} \end{cases}$$

В итоге получаем $\sum s_\alpha = \sum r_\alpha \pm 1$. Остается заметить, что для произвольных k и $l > k+1$ мы имеем

$$[i_k, i_l] = [i_k, i_{k+1}] \circ [i_{k+1}, i_l] \circ [i_{k+1}, i_k]$$

и таким образом каждая транспозиция $[i_k, i_l]$ раскладывается в композицию нечетного числа транспозиций "соседних" элементов. □

Определение. Четностью подстановки

$$\sigma = \begin{pmatrix} i_1 & i_2 & \cdots & i_{n-1} & i_n \\ j_1 & j_2 & \cdots & j_{n-1} & j_n \end{pmatrix}$$

называется четность суммы числа инверсий в первой и второй строках. Согласно предыдущей лемме четность подстановки не зависит от вида записи (при транспозиции столбцов меняется четность числа инверсий в обоих строках). Знаком σ называется

$$\operatorname{sgn}(\sigma) := (-1)^{\text{четность } (\sigma)}.$$

Пример. Согласно предыдущему примеру транспозиция является нечетной подстановкой.

Лекция 4

Четность произведения подстановок. Четность обратной подстановки. Число четных и нечетных подстановок. Группа A_n. Понятие подгруппы. Определители. Определитель треугольной матрицы. Определитель транспонированной матрицы. Вычисление определителя при помощи элементарных преобразований. Полилинейные и кососимметрические функции. Полилинейность и кососимметричность определителя.

Четность произведения подстановок. Четность обратной подстановки.

Предложение.

- $\operatorname{sgn}(\sigma_1 \circ \sigma_2) = \operatorname{sgn}(\sigma_1)\operatorname{sgn}(\sigma_2)$.
- $\operatorname{sgn}(\sigma^{-1}) = \operatorname{sgn}(\sigma)$.

Множество всех четных подстановок мы обозначим через A_n.

Предложение. *Число четных подстановок равно числу нечетных подстановок и равно $n!/2$.*

Доказательство. Зафиксируем некоторую нечетную подстановку τ (например, транспозицию). Согласно сказанному выше $\forall \sigma \in A_n \quad \tau \circ \sigma \in S_n \setminus A_n$. Следовательно, имеется отображение $f : A_n \to S_n \setminus A_n$, $f(\sigma) = \tau \circ \sigma$. Легко показать, что оно биективно. Следовательно, множества A_n и $S_n \setminus A_n$ равномощны. □

. . . . . .

Группа A_n. Понятие подгруппы.

. . . . . .

Определители

Определение. Пусть A – квадратная матрица

$$A = \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \cdots & \cdots & \cdots \\ a_{n,1} & \cdots & a_{n,n} \end{pmatrix}$$

Ее *определителем* называется число

$$|A| = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1,\sigma(1)} a_{2,\sigma(2)} \cdots a_{n,\sigma(n)}.$$

Пример. Пусть $n = 2$. Тогда S_n состоит из двух подстановок: тождественной ε и транспозиции $\tau = [1, 2]$. Поэтому

$$\begin{aligned} |A| = \begin{vmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{vmatrix} &= \operatorname{sgn}(\varepsilon)\, a_{1,\varepsilon(1)} a_{2,\varepsilon(2)} + \operatorname{sgn}(\tau)\, a_{1,\tau(1)} a_{2,\tau(2)} \\ &= a_{1,1} a_{2,2} - a_{1,2} a_{2,1}. \end{aligned}$$

Пример. Матрица $A = (a_{i,j})$ называется *верхнетреугольной*, если $a_{i,j} = 0$ при $i > j$ и она называется *нижнетреугольной*, если $a_{i,j} = 0$ при $i < j$. Покажем, что если $A = (a_{i,j})$ – верхнетреугольная (нижнетреугольная) матрица, то

$$|A| = a_{1,1} a_{2,2} \cdots a_{n,n}.$$

Действительно, в формуле для определителя член $a_{1,\sigma(1)} a_{2,\sigma(2)} \cdots a_{n,\sigma(n)}$ отличен от нуля только если $\sigma(i) \geq i \; \forall i$. Отсюда $\sigma(n) = n$ и поэтому $\sigma(n-1) \neq n$. Тогда $\sigma(n-1) = n-1$ и т. д. Получим, что единственный ненулевой член соответствует единичной подстановке.

Теорема. $|A| = |A^{\mathrm{T}}|$.

Доказательство. Заметим, что

$$\begin{pmatrix} \sigma(1) & \sigma(2) & \cdots & \sigma(n) \\ 1 & 2 & \cdots & n \end{pmatrix} = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma^{-1}(1) & \sigma^{-1}(2) & \cdots & \sigma^{-1}(n) \end{pmatrix}$$

Поэтому

$$\begin{aligned} |A^{\mathrm{T}}| &= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a^{\mathrm{T}}_{1,\sigma(1)} a^{\mathrm{T}}_{2,\sigma(2)} \cdots a^{\mathrm{T}}_{n,\sigma(n)} = \\ &= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{\sigma(1),1} a_{\sigma(2),2} \cdots a_{\sigma(n),n} = \\ &= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma^{-1}) a_{1,\sigma^{-1}(1)} a_{2,\sigma^{-1}(2)} \cdots a_{n,\sigma^{-1}(n)} = \\ &= \sum_{\tau \in S_n} \operatorname{sgn}(\tau) a_{1,\tau(1)} a_{2,\tau(2)} \cdots a_{n,\tau(n)} = |A|. \end{aligned}$$

□

Вычисление определителя при помощи элементарных преобразований.

Теорема. *Пусть матрица A' получена из матрицы A одним элементарным преобразованием. Тогда*

(I) $|A'| = |A|$;

($\text{II}_{\text{i},\lambda}$) $|A'| = \lambda|A|$;

(III) $|A'| = -|A|$.

Доказательство. ..... □

Функция $F(X_1, \ldots, X_N)$ от нескольких аргументов называется *полилинейной*, если при подстановке вместо любой переменной X_i значения $\lambda' X_i' + \lambda'' X_i''$, где λ' и λ'' – произвольные числа, мы имеем

$$F(X_1, \ldots, \lambda' X_i' + \lambda'' X_i'', \ldots, X_N) =$$

$$= \lambda' F(X_1, \ldots, X_i', \ldots, X_N) + \lambda'' F(X_1, \ldots, X_i'', \ldots, X_N)$$

Рассмотрим матрицу A как совокупность ее строк

$$A = \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \ldots\ldots\ldots\ldots \\ a_{n,1} & \cdots & a_{n,n} \end{pmatrix} = (A_1, \ldots, A_n), \qquad A_i = \begin{pmatrix} a_{i,1} & \cdots & a_{i,n} \end{pmatrix}$$

а определитель $|A|$ рассмотрим как числовую функцию строк

$$|A| = |A_1, \ldots, A_n| = F(A_1, \ldots, A_n).$$

Теорема (полилинейность определителя)**.** *Определитель является полилинейной функцией своих строк.*

Доказательство. Пусть $A_i = \lambda' A_i' + \lambda'' A_i''$, где

$$A_i' = \begin{pmatrix} a_{i,1}' & a_{i,2}' & \ldots & a_{i,n}' \end{pmatrix} \qquad A_j'' = \begin{pmatrix} a_{i,1}'' & a_{i,2}'' & \ldots & a_{i,n}'' \end{pmatrix}$$

Таким образом, $a_{i,j} = \lambda' a_{i,j}' + \lambda'' a_{i,j}'' \quad \forall j$. Поэтому

$$|A| = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1,\sigma(1)} \cdots a_{i,\sigma(i)} \cdots a_{n,\sigma(n)} =$$

$$= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1,\sigma(1)} \cdots (\lambda' a_{i,\sigma(i)}' + \lambda'' a_{i,\sigma(i)}'') \cdots a_{n,\sigma(n)} =$$

$$= \lambda' \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1,\sigma(1)} \cdots a_{i,\sigma(i)}' \cdots a_{n,\sigma(n)} +$$

$$\lambda'' \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1,\sigma(1)} \cdots a_{i,\sigma(i)}'' \cdots a_{n,\sigma(n)} = \lambda' |A'| + \lambda'' |A''|,$$

где A' (соотв. A'') – матрица, составленная из строк $A_1, \ldots, A_i', \ldots, A_n$ (соотв. $A_1, \ldots, A_i'', \ldots, A_n$). □

Функция $F(X_1, \ldots, X_N)$ от нескольких аргументов называется *кососимметрической*, если при подстановке двух любых переменных X_i и X_i, $i \neq j$ функция меняет знак:

$$F(X_1, \ldots, X_i, \ldots, X_j, \ldots, X_N) =$$

$$= -F(X_1, \ldots, X_j, \ldots, X_i, \ldots, X_N).$$

Лемма. *Если $F(X_1, \ldots, X_N)$ – полилинейная функция такая, что $F(X_1, \ldots, X_i, \ldots, X_j, \ldots, X_N) = 0$ при $X_i = X_i, \quad \forall i, j,\ i \neq j$, то эта функция является кососимметрической.*

Доказательство. ..... □

Теорема (кососимметричность определителя)**.** *Определитель является кососимметрической функцией своих строк.*

Доказательство. Пусть $A_i = A_j$, т.е. $a_{i,k} = a_{j,k} \quad$ для любого k, где $i < j$. Докажем, что $|A| = 0$. Разобьём все подстановки из S_n на (непересекающиеся) пары

$$\sigma \qquad\qquad \sigma' = \sigma \circ [i, j]$$

Так как $a_{i,\sigma(i)} = a_{j,\sigma(i)}$ и $a_{j,\sigma(j)} = a_{i,\sigma(j)}$, то соответствующие члены в формуле для определителя

$$\operatorname{sgn}(\sigma) a_{1,\sigma(1)} \cdots a_{i,\sigma(i)} \cdots a_{j,\sigma(j)} \cdots a_{n,\sigma(n)}$$

$$-\operatorname{sgn}(\sigma) a_{1,\sigma(1)} \cdots a_{i,\sigma(j)} \cdots a_{j,\sigma(i)} \cdots a_{n,\sigma(n)}$$

сокращаются. □

Лекция 5

Эквивалентное определение определителя (как полилинейной кососимметрической формы). Определитель с углом нулей. Разложение определителя по строке (и фальшивое разложение). Определитель Вандермонда. Теорема Крамера.

Эквивалентное определение определителя (как полилинейной кососимметрической формы)

. . . . . .

Определитель с углом нулей

Говорят, что квадратная матрица

$$A = \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \cdots & \cdots & \cdots \\ a_{n,1} & \cdots & a_{n,n} \end{pmatrix}$$

имеет нижний *угол нулей* если для некоторого $1 \leq k \leq n$ имеем $a_{i,j}$ при $i > k$, $j \leq k$. Аналогично определяется матрица с верхним углом нулей. Таким образом, матрица с нижним углом нулей может быть записана в виде

$$(*) \qquad A = \begin{pmatrix} A_1 & B \\ 0 & A_2 \end{pmatrix}$$

где A_1 и A_2 – квадратные матрицы размеров $k \times k$ и $(n-k) \times (n-k)$, соответственно, B – матрица размера $k \times (n-k)$, а 0 – нулевая матрица размера $(n-k) \times k$.

Теорема. *Пусть A – матрица с нижним углом нулей, записанная как выше. Тогда $|A| = |A_1||A_2|$.*

Доказательство. Приведем матрицу A_1 (соотв. A_2) элементарными преобразованиями строк типа (I) к ступенчатой матрице A_1' (соотв. A_2'). Тогда $|A_1| = |A_1'|$ и $|A_2| = |A_2'|$. Пусть матрица A' получена из A выполнением соответствующих элементарных преобразований строк (т.е. над первыми k строками матрицы A мы выполняем те же преобразования, что и над строками A_1, а над следующими $n-k$ строками матрицы A мы

выполняем те же преобразования, что и над строками A_2). Тогда $|A'| = |A|$ и поэтому достаточно доказать, что $|A'| = |A'_1||A'_2|$. Ясно, что

$$A' = \begin{pmatrix} A'_1 & B' \\ 0 & A'_2 \end{pmatrix}$$

Матрицы A'_1 и A'_2 – треугольные (ниже главной диагонали стоят нули) и таковой же является A'. В этом случае равенство $|A'| = |A'_1||A'_2|$ следует из того, что определитель треугольной матрицы равен произведению элементов на ее диагонали. □

Следствие. *Пусть A – матрица с верхним углом нулей, записанная в виде*

$$A = \begin{pmatrix} A_1 & 0 \\ B & A_2 \end{pmatrix}$$

Тогда $|A| = |A_1||A_2|$.

Пусть $A = (a_{i,j})$ – $n \times m$-матрица. *Минором* порядка r (где $1 \le r \le n$ и $1 \le r \le m$) называется определитель матрицы из элементов, стоящих на пересечении некоторых r строк и r столбцов матрицы A. Если теперь $A = (a_{i,j})$ – $n \times n$-матрица, то через $M_{i,j}$ мы будем обозначать минор порядка $n-1$, полученный из A вычеркиванием i-ой строки и j-ого столбца. В этом случае *алгебраическим дополнением* к элементу $a_{i,j}$ называется число $A_{i,j} := (-1)^{i+j} M_{i,j}$.

Теорема (разложение определителя по строке)**.**

$$\sum_{j=1}^{n} a_{i,j} A_{k,j} = 0 \quad \textit{при } k \ne i.$$

Доказательство. Пусть $S = (a_{i,1}, \ldots, a_{i,n})$ – i-ая строка матрицы и пусть $S_j = (0, \ldots, a_{i,j}, \ldots, 0)$. Тогда $S = \sum S_i$. Пусть B_j – матрица, полученная из A заменой S на S_j. Согласно свойству полилинейности $|A| = \sum |B_j|$, где

$$|B_j| = \begin{vmatrix} a_{1,1} & \cdots & a_{1,j} & \cdots & a_{1,n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & a_{1,j} & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{n,1} & \cdots & a_{n,j} & \cdots & a_{n,n} \end{vmatrix} = (-1)^{i+j-2} \begin{vmatrix} a_{i,j} & 0 & \cdots & 0 \\ a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ \cdots & \cdots & & \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \end{vmatrix}$$

Последний определитель имеет верхний угол нулей. Поэтому $|B_j| = (-1)^{i+j} M_{i,j}$. □

Теорема (фальшивое разложение по строке)**.**

$$|A| = \sum_{j=1}^{n} a_{i,j} A_{i,j}$$

Доказательство. Рассмотрим матрицу

$$A' = (a'_{r,j}), \quad \text{где} \quad a'_{r,j} = \begin{cases} a_{r,j} & \text{при } r \neq k \\ a_{i,j} & \text{при } r = k \end{cases}$$

Мы в матрице A заменили k-ую строку на i-ю. Таким образом, в A' строки с номерами k и i совпадают. Поэтому $|A'| = 0$. Разлагая A' по k-й строке получим

$$0 = |A'| = \sum_{j=1}^{n} a'_{k,j} A'_{k,j} = \sum_{j=1}^{n} a_{i,j} A_{k,j}.$$

□

Теорема (Теорема Крамера). *Рассмотрим квадратную систему линейных уравнений*

$$\begin{cases} a_{1,1}x_1 + \cdots + a_{1,n} = b_1 \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ a_{n,1}x_1 + \cdots + a_{n,n} = b_n \end{cases}$$

Положим

$$\Delta := \begin{vmatrix} a_{1,1} & \cdots & a_{1,n} \\ \cdots\cdots & \cdots & \cdots\cdots \\ a_{n,1} & \cdots & a_{n,n} \end{vmatrix} \qquad \Delta_i := \begin{vmatrix} a_{1,1} & \cdots & b_1 & \cdots & a_{1,n} \\ \cdots\cdots & \cdots & \cdots & \cdots & \cdots\cdots \\ a_{n,1} & \cdots & b_n & \cdots & a_{n,n} \end{vmatrix}$$

Тогда

(1) *система совместна и определена* $\iff \Delta \neq 0$,

(2) *если* $\Delta \neq 0$, *то решение системы имеет вид* $x_i = \Delta_i/\Delta$.

Доказательство. (2) Положим $\alpha_j := \Delta_j/\Delta$. Тогда

$$\sum_{j=1}^{n} a_{i,j}\alpha_j = \frac{1}{\Delta}\sum_{j=1}^{n} a_{i,j}\Delta_j = \frac{1}{\Delta}\sum_{j=1}^{n} a_{i,j}\sum_{k=1}^{n} b_k A_{k,j} =$$

$$= \frac{1}{\Delta}\sum_{k=1}^{n} b_k \sum_{j=1}^{n} a_{i,j}A_{k,j} = \frac{b_i\Delta}{\Delta} = b_i$$

поскольку

$$\sum_{j=1}^{n} a_{i,j}A_{k,j} = \begin{cases} \Delta & \text{если } k = i \\ 0 & \text{если } k \neq i \end{cases}$$

Таким образом, $\Delta \neq 0 \Longrightarrow$ система совместна и $x_i = \Delta_i/\Delta$ – решение.

(1) Приведем матрицу системы элементарными преобразованиями строк к ступенчатому виду:

$$\begin{pmatrix} a_{1,1} & \cdots & a_{1,n} & b_1 \\ \cdots\cdots & \cdots & \cdots\cdots & \cdots \\ a_{n,1} & \cdots & a_{n,n} & b_n \end{pmatrix} \longmapsto \begin{pmatrix} a'_{1,1} & \cdots & a'_{1,n} & b'_1 \\ \cdots\cdots & \cdots & \cdots\cdots & \cdots \\ 0 & \cdots & a'_{n,n} & b'_n \end{pmatrix}$$

Ясно, что $\Delta \neq 0 \iff \Delta' \neq 0 \iff a'_{i,i} \neq 0$ для любого $i \iff$ система совместна и определена. □

Теорема (Определитель Вандермонда).

$$\Delta_n = \begin{vmatrix} 1 & a_1 & a_1^2 & \cdots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \cdots & a_2^{n-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & a_n & a_n^2 & \cdots & a_n^{n-1} \end{vmatrix} = \prod_{1 \le j < i \le n} (a_i - a_j).$$

Доказательство. Индукция по n. $n = 2$: $\Delta_2 = a_2 - a_1$. Шаг индукциии.

$$\Delta_n = \begin{vmatrix} 1 & a_1 - a_n & a_1^2 - a_1 a_n & \cdots & a_1^{n-1} - a_1^{n-2} a_n \\ 1 & a_2 - a_n & a_2^2 - a_2 a_n & \cdots & a_2^{n-1} - a_2^{n-2} a_n \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & a_{n-1} - a_n & a_{n-1}^2 - a_{n-1} a_n & \cdots & a_{n-1}^{n-1} - a_{n-1}^{n-2} a_n \\ 1 & 0 & 0 & \cdots & 0 \end{vmatrix} =$$

$$= (-1)^{n+1} \begin{vmatrix} a_1 - a_n & a_1^2 - a_1 a_n & \cdots & a_1^{n-1} - a_1^{n-2} a_n \\ a_2 - a_n & a_2^2 - a_2 a_n & \cdots & a_2^{n-1} - a_2^{n-2} a_n \\ \cdots & \cdots & \cdots & \cdots \\ a_{n-1} - a_n & a_{n-1}^2 - a_{n-1} a_n & \cdots & a_{n-1}^{n-1} - a_{n-1}^{n-2} a_n \end{vmatrix} =$$

$$= (-1)^{n+1} (a_1 - a_n)(a_2 - a_n) \cdots (a_{n-1} - a_n) \begin{vmatrix} 1 & a_1 & \cdots & a_1^{n-2} \\ 1 & a_2 & \cdots & a_2^{n-2} \\ \cdots & \cdots & \cdots & \cdots \\ 1 & a_{n-1} & \cdots & a_{n-1}^{n-2} \end{vmatrix} =$$

$$= (a_n - a_1)(a_n - a_2) \cdots (a_n - an - 1) \Delta_{n-1}.$$

□

Лекция 6

Определитель произведения матриц. Обратная матрица. Единицы и обратные элементы в ассоциативном кольце (единственность). Критерий существования обратной матрицы. Формула для обратной матрицы. Вычисление обратной матрицы при помощи элементарных преобразований. Делители нуля в кольце. Делители нуля в кольце матриц.

Лемма. (1) *Если* $|A| \neq 0$, *то* $A = U_1 \cdots U_m$, *где* $U_1, \ldots U_m$ – *элементарные матрицы.*

(2) *Если* $|A| = 0$, *то* $A = U_1 \cdots U_m A'$, *где* A' – *матрица с нулевой строкой, а* $U_1, \ldots U_m$ – *элементарные матрицы.*

Лемма. *Если* U – *элементарная матрица, то*

$$|U \cdot A| = |U| \cdot |A|.$$

Следствие. *Если* $U_1, \ldots U_m$ – *элементарные матрицы, то*

$$|U_1 \cdots U_m \cdot A| = |U_1 \cdots U_m| \cdot |A|.$$

Теорема. *Пусть* A, $B \in \mathrm{Mat}_n(\Bbbk)$. *Тогда* $|A| \cdot |B| = |A \cdot B|$.

Доказательство. Предположим, что $|A| = 0$. Запишем $A = U_1 \cdots U_m A'$, где A' – матрица с нулевой строкой, а $U_1, \ldots U_m$ – элементарные матрицы. Тогда $A'B$ также имеет нулевую строку. Значит

$$|A \cdot B| = |(U_1 \cdots U_m \cdot A') \cdot B| = |U_1 \cdots U_m| \cdot |A' \cdot B| = 0 = |A| \cdot |B|.$$

Пусть $|A| \neq 0$. Тогда $A = U_1 \cdots U_m$, где $U_1, \ldots U_m$ – элементарные матрицы и

$$|A \cdot B| = |(U_1 \cdots U_m) \cdot B| = |U_1 \cdots U_m| \cdot |\cdot B| = |A| \cdot |B|. \qquad \square$$

. . . . . .

Предложение. *Пусть* R – *ассоциативное кольцо.*

(1) *Если единичный элемент существует, то он единственный.*

(2) *Если для* $a \in R$ *существует обратный элемент, то он единственный.*

(3) *Если элемент* $a \in R$ *обратим, то он не может быть делителем нуля.*

(4) *Если элемент* $a \in R$ *обратим, то элемент* a^{-1} *обратим и* $(a^{-1})^{-1} = a$.

(5) *Если элементы* a, $b \in R$ *обратимы, то элемент* $b \cdot a$ *обратим и* $(b \cdot a)^{-1} = a^{-1} \cdot b^{-1}$.

Обратная матрица

Присоединенной матрицей к матрице $A = (a_{i,j})$ называется матрица $\hat{A} = (\hat{a}_{i,j})$, где $\hat{a}_{i,j} = A_{j,i}$. Таким образом,

$$\hat{A} = \begin{pmatrix} A_{1,1} & \cdots & A_{n,1} \\ \cdots & \cdots & \cdots \\ A_{1,n} & \cdots & A_{n,n} \end{pmatrix}$$

Теорема (Формула для обратной матрицы)**.** *Пусть* $A \in \mathrm{Mat}_n(\Bbbk)$. *Если* $|A| \neq 0$, *то обратная матрица существует и* $A^{-1} = \frac{1}{|A|}\hat{A}$.

Доказательство. Пусть $A \cdot \hat{A} = (c_{i,j})$. Тогда

$$c_{i,j} = \sum_{k=1}^{n} a_{i,k}\hat{a}_{k,j} = \sum_{k=1}^{n} a_{i,k}A_{j,k} = \begin{cases} |A| & \text{если } i = j, \\ 0 & \text{если } i \neq j. \end{cases}$$

Таким образом, $A \cdot \hat{A} = |A|E$. Аналогично, $\hat{A} \cdot A = |A|E$. □

Следствие (Критерий обратимости матрицы)**.** $|A| \neq 0 \iff \exists A^{-1}$.

Пример. Пусть $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Тогда

$$A = \begin{pmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{pmatrix}.$$

Вычисление обратной матрицы при помощи элементарных преобразований

. . . . . .

Замечание. Матрица обратная к элементарной – также элементарная: $U_{i,j,\lambda} \cdot U_{i,j,-\lambda} = E$, $U_{i,\lambda} \cdot U_{i,\lambda^{-1}} = E$, $U_{i,j} \cdot U_{i,j} = E$.

Теорема (делители нуля в кольце матриц)**.** *Пусть* $A \in \mathrm{Mat}_n(\Bbbk)$, $A \neq 0$. *Следующие условия эквивалентны:*

(1) $|A| = 0$,

(2) A – *левый делитель нуля в* $\mathrm{Mat}_n(\Bbbk)$,

(3) A – *правый делитель нуля в* $\mathrm{Mat}_n(\Bbbk)$,

(4) *не существует обратной матрицы к* A.

Матрицы, удовлетворяющие этим условиям, называются *вырожденными*.

Доказательство. (1) $\Longrightarrow$ (2) Пусть $|A| = 0$. По теореме Крамера существует столбец X такой, что $A \cdot X = 0$. Пусть $B \in \mathrm{Mat}_n(\Bbbk)$ – матрица у которой первый столбец совпадает с X, а остальные столбцы – нулевые. Тогда $A \cdot B = 0$.

(1) $\Longrightarrow$ (3) Пусть $|A| = 0$. Тогда $|A^{\mathrm{T}}| = 0$ и A^{T} – левый делитель нуля, т.е. $A^{\mathrm{T}} \cdot B = 0$. Отсюда $B^{\mathrm{T}} \cdot A = 0$.

(2)$\Longrightarrow$ (4) Иначе $A \cdot B = 0$, $0 = A^{-1} \cdot A \cdot B = B$.

(3) $\Longrightarrow$ (4) Аналогично.

(4) $\Longrightarrow$ (1) Иначе $|A| \neq 0$ и обратная матрица существует по формуле для обратной матрице. $\square$

Следствие. *Любая невырожденная матрица является произведением элементарных.*

. . . . . .

Лекция 7

Невырожденные матрицы. Группы $GL_n(\mathbb{R})$ и $SL_n(\mathbb{R})$. Векторные пространства. Линейная зависимость. Критерий невырожденности матрицы. Базис. Координаты. Лемма о линейной зависимости. Следствия.

Векторные пространства.

Определение. *Векторным пространством* над полем $\Bbbk$ называется множество V, а котором задана операция сложения элементов V между собой

$$\forall \mathbf{v},\, \mathbf{w} \in V, \quad \text{задан элемент } \mathbf{v}+\mathbf{w} \in V$$

и операция умножения элементов $\Bbbk$ на элементы V

$$\forall \lambda \in \Bbbk \quad \forall \mathbf{v} \in V, \quad \text{задан элемент } \lambda\mathbf{v} \in V,$$

такие, что выполняются следующие свойства:

(I) (1) $\mathbf{v}+(\mathbf{w}+\mathbf{u}) = (\mathbf{v}+\mathbf{w})+\mathbf{u}, \quad \forall \mathbf{v},\, \mathbf{w},\, \mathbf{u} \in V;$

(2) $\exists \mathbf{0} \in V \quad \mathbf{v}+\mathbf{0} = \mathbf{0}+\mathbf{v} = \mathbf{v}, \quad \forall \mathbf{v} \in V;$

(3) $\forall \mathbf{v} \in V \quad \exists -\mathbf{v} \in V \quad \mathbf{v}+(-\mathbf{v}) = (-\mathbf{v})+\mathbf{v} = \mathbf{0};$

(4) $\mathbf{v}+\mathbf{w} = \mathbf{w}+\mathbf{v}, \quad \forall \mathbf{v},\, \mathbf{w} \in V.$

(II) (1) $(\alpha+\beta)\mathbf{v} = \alpha\mathbf{v}+\beta\mathbf{v}, \quad \forall \mathbf{v} \in V, \forall \alpha,\, \beta \in \Bbbk;$

(2) $\alpha(\mathbf{v}+\mathbf{w}) = \alpha\mathbf{v}+\alpha\mathbf{w}\ , \quad \forall \mathbf{v},\, \mathbf{w} \in V, \forall \alpha \in \Bbbk;$

(3) $(\alpha\beta)\mathbf{v} = \alpha(\beta\mathbf{v}), \quad \forall \mathbf{v} \in V, \forall \alpha,\, \beta \in \Bbbk;$

(4) $1 \cdot \mathbf{v} = \mathbf{v}, \quad \forall \mathbf{v} \in V.$

При этом элементы V называются *векторами*, а элементы $\Bbbk$ – *скалярами*.

Замечание. Непосредственно из определения получаем.

- Для любых $\mathbf{a},\, \mathbf{b} \in V$ уравнение $\mathbf{a}+\mathbf{x} = \mathbf{b}$ имеет единственное решение.
- Нулевой элемент $\mathbf{0} \in V$ единственен.
- Для любого $\mathbf{a} \in V$ противоположный элемент $-\mathbf{a}$ единственен.

- Для любого $\mathbf{a} \in V$ имеем $0\mathbf{a} = \mathbf{0}$. Действительно, $\mathbf{a} + 0\mathbf{a} = 1\mathbf{a} + 0\mathbf{a} = (1+0)\mathbf{a} = 1\mathbf{a} = \mathbf{a}$.
- Для любого $\alpha \in \Bbbk$ имеем $\alpha\mathbf{0} = \mathbf{0}$. Действительно, $\alpha\mathbf{0} + \alpha\mathbf{a} = \alpha(\mathbf{0} + \mathbf{a}) = \alpha\mathbf{a}$.

Примеры. (1) $V = \{0\}$.

(2) Пусть $\mathbb{R}^n = \{(\alpha_1, \ldots, \alpha_n)\}$ – множество строк длины n, где $\alpha_i \in \mathbb{R}$. Сложение и умножение на числа – покомпонентные. Аналогично определяется $\mathbb{Q}^n$ ...

(3) множество $\mathrm{Mat}_{n,m}(\Bbbk)$ всех $n \times m$-матриц;

(4) геометрические векторы в двумерном (соотв. трехмерном) пространстве;

(5) множество всех (бесконечных) последовательностей a_n;

(6) множество всех числовых функций на отрезке.

Определение. Пусть $\mathbf{a}_1, \ldots, \mathbf{a}_m \in V$ и пусть $\alpha_1, \ldots, \alpha_m \in \Bbbk$. *Линейной комбинацией* векторов $\mathbf{a}_1, \ldots, \mathbf{a}_m \in V$ с коэффициентами $\alpha_1, \ldots, \alpha_m \in \Bbbk$ называется $\alpha_1\mathbf{a}_1 + \cdots + \alpha_m\mathbf{a}_m \in V$. Линейная комбинация называется *тривиальной*, если $\alpha_1 = \cdots = \alpha_m = 0$.

Определение. Векторы $\mathbf{a}_1, \ldots, \mathbf{a}_m \in V$ называются *линейно зависимыми*, если их некоторая нетривиальная линейная комбинация равна нулю: $\alpha_1\mathbf{a}_1 + \cdots + \alpha_m\mathbf{a}_m = \mathbf{0}$, где $\alpha_i \neq 0$ для некоторого i. В противном случае векторы называются *линейно независимыми*. Это условие можно переформулировать следующим образом:

- $\alpha_1\mathbf{a}_1 + \cdots + \alpha_m\mathbf{a}_m = \mathbf{0} \Longrightarrow \alpha_1 = \cdots = \alpha_m = 0$ (если линейная комбинация равна нулю, то она тривиальна).

Примеры. (1) Один вектор $\mathbf{a}_1$ линейно зависим $\Longleftrightarrow \mathbf{a}_1 = \mathbf{0}$.

(2) Если $\mathbf{a}_i = \mathbf{0}$, то система $\mathbf{a}_1, \ldots, \mathbf{a}_m$ линейно зависима.

(3) Два вектора $\mathbf{a}_1$, $\mathbf{a}_2$ линейно зависимы $\Longleftrightarrow$ они пропорциональны: или $\mathbf{a}_1 = \lambda\mathbf{a}_2$ или $\mathbf{a}_2 = \lambda\mathbf{a}_1$ для некоторого $\lambda \in \Bbbk$.

Замечание. (1) Если подсистема $\{\mathbf{a}_{i_1}, \ldots, \mathbf{a}_{i_k}\} \subset \{\mathbf{a}_1, \ldots, \mathbf{a}_m\}$ линейно зависима, то и вся система $\{\mathbf{a}_1, \ldots, \mathbf{a}_m\}$ линейно зависима.

(2) Если система $\{\mathbf{a}_1, \ldots, \mathbf{a}_m\}$ линейно независима, то и любая ее подсистема $\{\mathbf{a}_{i_1}, \ldots, \mathbf{a}_{i_k}\} \subset \{\mathbf{a}_1, \ldots, \mathbf{a}_m\}$ линейно независима.

Предложение. *Система векторов $\mathbf{a}_1, \ldots, \mathbf{a}_m \in V$ линейно зависима $\Longleftrightarrow$ некоторый ее вектор $\mathbf{a}_j$ выражается как линейная комбинация остальных.*

Доказательство. ..... □

Теорема (Критерий невырожденности матрицы)**.** *Пусть A – квадратная матрица. Следующие условия эквивалентны:*

(1) *A невырождена;*

(2) *столбцы A линейно независимы;*

(3) *строки A линейно независимы.*

Доказательство. Пусть $A_1, \dots, A_n$ – столбцы матрицы. Запишем условие линейной зависимости $\lambda_1 A_1 + \dots + \lambda_n A_n = 0$, где $\lambda_i \in \Bbbk$, а 0 – нулевой столбец. Условие может быть переписано в виде

$$A \cdot \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

Это однородная система линейных уравнений. По теореме Крамера $|A| \neq 0 \iff$ система определена (т.е. $\lambda_1 = \dots = \lambda_n = 0$ – единственное решение) $\iff$ столбцы $A_1, \dots, A_n$ линейно независимы. Это доказывает (1) $\iff$ (2). Так как $|A| = |A^{\mathrm{T}}|$, то аналогично получаем (1) $\iff$ (3). □

Определение. Пусть V – векторное пространство и пусть $M \subset V$ – любое подмножество (система векторов). Говорят, что элементы $\mathbf{e}_1, \dots, \mathbf{e}_m \in M$ образуют *базис M*, если

(1) векторы $\mathbf{e}_1, \dots, \mathbf{e}_m$ линейно независимы,

(2) для любого $\mathbf{v} \in M$ векторы $\mathbf{v}, \mathbf{e}_1, \dots, \mathbf{e}_m$ линейно зависимы.

Базисом пространства V называется базис $M = V$.

Замечание. Элементы $\mathbf{e}_1, \dots, \mathbf{e}_m \in M$ образуют базис тогда и только тогда, когда выполнены условия (1) и (2)′:

(2)′ любой вектор $\mathbf{v} \in M$ линейно выражается через $\mathbf{e}_1, \dots, \mathbf{e}_m$.

Замечание. Мы рассматриваем только базисы из конечного числа элементов.

Замечание. Базис рассматривается как упорядоченное множество.

Пример. В пространстве $\mathbb{R}^n$ имеется стандартный базис $\mathbf{e}_1, \dots, \mathbf{e}_n$, где $\mathbf{e}_i = (0, \dots, \underset{\substack{\uparrow \\ i}}{1}, \dots, 0)$.

Предложение. *Пусть $\mathbf{e}_1, \dots, \mathbf{e}_m \in M$ – базис. Тогда любой вектор $\mathbf{v} \in M$ однозначно выражается через $\mathbf{e}_1, \dots, \mathbf{e}_m$. Коэффициенты этого разложения называются* координатами *вектора.*

Доказательство. ..... □

Теорема (лемма о линейной зависимости)**.** *Пусть векторы $\mathbf{v}_1, \dots, \mathbf{v}_n$ линейно независимы и линейно выражаются через векторы $\mathbf{w}_1, \dots, \mathbf{w}_m$. Тогда $n \leq m$.*

Доказательство. Предположим, что $n > m$. Запишем

$$\mathbf{v}_j = \alpha_{1,j}\mathbf{w}_1 + \cdots + \alpha_{m,j}\mathbf{w}_m.$$

Тогда

$$\sum_{j=1}^{n} \lambda_j \mathbf{v}_j = \sum_{j=1}^{n} \lambda_j \left(\sum_{i=1}^{m} \alpha_{i,j}\mathbf{w}_i \right) = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} \alpha_{i,j}\lambda_j \right) \mathbf{w}_i.$$

Рассмотрим систему однородных линейных уравнений

$$\sum_{j=1}^{n} \alpha_{i,j}\lambda_j = 0, \quad i = 1, \ldots m.$$

относительно $\lambda_1, \ldots, \lambda_n$. Так как число неизвестных меньше числа уравнений, то система имеет ненулевое решение такое, что $\sum_{j=1}^{n} \lambda_j \mathbf{v}_j = \mathbf{0}$. □

Следствие. *Любой базис $M \subset V$ содержит одинаковое количество элементов. Более точно, если $\mathbf{w}_1, \ldots, \mathbf{w}_m$ – базис M, то любая система из n векторов $\mathbf{v}_1, \ldots, \mathbf{v}_n \in M$ при $n > m$ линейно зависима. Если же $\mathbf{v}_1, \ldots, \mathbf{v}_n$ также образуют базис M, то $m = n$.*

Доказательство. Векторы $\mathbf{v}_1, \ldots, \mathbf{v}_n$ линейно выражаются через $\mathbf{w}_1, \ldots, \mathbf{w}_m$. Если $\mathbf{v}_1, \ldots, \mathbf{v}_n$ линейно независимы, то по лемме о линейной зависимости $n \leq m$. Если же $\mathbf{v}_1, \ldots, \mathbf{v}_n$ образуют базис, то аналогично получаем $m \leq n$. □

Определение. Если $M \subset V$ – любое подмножество, то *рангом* M (обозначается $\operatorname{rk} M$) называется число элементов базиса (если конечный базис существует). Рангом столбцов матрицы называется ранг системы ее столбцов (как системы векторов $\mathbb{R}^n$). Рангом строк матрицы называется ранг системы ее строк*. *Размерностью*† пространства V (обозначается $\dim V$) называется ранг $M = V$.

Замечание. Если $M \subset V$, то $\operatorname{rk} M$ равен максимальному числу линейно независимых векторов $\mathbf{v}_1, \ldots, \mathbf{v}_n \in M$.

Следствие. *Пусть $\dim V = n$. Тогда система из m векторов в V линейно зависима при $m > n$.*

Следствие. *Если все векторы системы $M \subset V$ линейно выражаются через векторы системы $M' \subset V$, то $\operatorname{rk} M \leq \operatorname{rk} M'$.*

Доказательство. Пусть $\mathbf{v}_1, \ldots, \mathbf{v}_n$ – базис M, а $\mathbf{v}'_1, \ldots, \mathbf{v}'_m$ – базис M'. По условию векторы $\mathbf{v}_1, \ldots, \mathbf{v}_n$ линейно выражаются через векторы M', а любой вектор M' линейно выражается через $\mathbf{v}'_1, \ldots, \mathbf{v}'_m$. Следовательно, $\mathbf{v}_1, \ldots, \mathbf{v}_n$ линейно выражаются через $\mathbf{v}'_1, \ldots, \mathbf{v}'_m$. По лемме о линейной зависимости $n \leq m$. □

*Позже мы докажем, что для любой матрицы ранги строк и столбцов совпадают.

†Термин *ранг* употребляется в отношении подмножества (чаще всего конечного) $M \subset V$. Термин *размерность* употребляется только в отношении векторного пространства.

Следствие. *Пусть* $\dim V = n$, $M \subset V$ *и пусть* $\mathbf{e}_1, \ldots, \mathbf{e}_k \in M$ *– линейно независимые векторы. Тогда* $\mathbf{e}_1, \ldots, \mathbf{e}_k \in M$ *можно дополнить до базиса* M.

Доказательство. Если для любого $\mathbf{x} \in M$ векторы $\mathbf{e}_1, \ldots, \mathbf{e}_k, \mathbf{x}$ линейно зависимы, то $\mathbf{e}_1, \ldots, \mathbf{e}_k$ – базис M. В противном случае существует $\mathbf{x} \in M$ такой, что векторы $\mathbf{e}_1, \ldots, \mathbf{e}_k, \mathbf{x}$ линейно независимы. Полагаем $\mathbf{e}_{k+1} = \mathbf{x}$ и продолжаем процесс. Процесс оборвется поскольку число линейно независимых векторов не превосходит n. □

Следствие. *Пусть* $W \subset V$ *– подпространство векторного пространства. Тогда* $\dim W \leq \dim V$ *и если* $\dim W = \dim V$, *то* $W = V$.

Доказательство. Первое неравенство следует из предыдущего следствия (полагаем $M' = V$, $M = W$).

Пусть $\dim W = \dim V$. Докажем[‡], что $W = V$. Пусть $\mathbf{v}_1, \ldots, \mathbf{v}_n$ – базис V и пусть $\mathbf{w}_1, \ldots, \mathbf{w}_n$ – базис W. Так как $w_i \in V$, то мы можем записать

$$\mathbf{w}_i = \sum_{j=1}^{n} a_{i,j}\mathbf{v}_j.$$

Если матрица $A = (a_{i,j})$ вырождена, то ее строки линейно зависимы: $\sum_{i=1}^{n} \lambda_i a_{i,j} = 0$ $\forall j$. Но тогда

$$\sum_{i=1}^{n} \lambda_i \mathbf{w}_i = \sum_{i=1}^{n} \lambda_i \left(\sum_{j=1}^{n} a_{i,j}\mathbf{v}_j \right) = \sum_{j=1}^{n} \left(\sum_{i=1}^{n} \lambda_i a_{i,j} \right) \mathbf{v}_j = 0.$$

Противоречие показывает, что матрица $A = (a_{i,j})$ невырождена. Следовательно, существует обратная матрица $A^{-1} = (b_{i,j})$. Имеем

$$\sum_{i=1}^{n} b_{k,j}\mathbf{w}_i = \sum_{i=1}^{n} b_{k,i} \left(\sum_{j=1}^{n} a_{i,j}\mathbf{v}_j \right) =$$

$$= \sum_{j=1}^{n} \left(\sum_{i=1}^{n} b_{k,i}a_{i,j} \right) \mathbf{v}_j = \sum_{j=1}^{n} \delta_{k,j}\mathbf{v}_j = \mathbf{v}_k.$$

т.е. $\mathbf{v}_k \in W \quad \forall k$. Поэтому $V \subset W$. □

Другое доказательство. Система $\mathbf{w}_1, \ldots, \mathbf{w}_n \in W \subset V$ может быть дополнена до базиса V. Так как $\dim V = n$, то $\mathbf{w}_1, \ldots, \mathbf{w}_n$ – уже базис V. Следовательно, $V \subset W$. □

[‡]Имеется короткое доказательство (см. ниже)

Лекция 8

Ранг матрицы. Ранг суммы матриц. Теорема о ранге. Алгоритм нахождения базиса. Ранг произведения матриц. Критерий совместности системы линейных уравнений. Решения однородной системы линейных уравнений. Фундаментальная система решений. Задание подпространства системой линейных уравнений.

Теорема (Теорема о ранге матрицы)**.** *Ранг системы строк матрицы равен рангу системы ее столбцов и равен наивысшему порядку отличного от нуля минора.*

Лемма. *Ранг (системы строк) матрицы не меняется при элементарных преобразованиях строк.*

Доказательство. Пусть матрица A' получена из матрицы A одним элементарным преобразованием строк. Тогда строка матрицы A' линейно выражаются через строки матрицы A. Следовательно, $\operatorname{rk} A' \leq \operatorname{rk} A$. Преобразование $A \mapsto A'$ обратимо, поэтому $\operatorname{rk} A \leq \operatorname{rk} A'$. □

Лемма. *При элементарных преобразованиях строк матрицы линейные зависимости (независимости) системы ее столбцов не меняются.*

Доказательство. Пусть $A = (a_{i,j})$ – $n \times m$-матрица и пусть $A_1, \ldots, A_m$ – ее столбцы. Пусть матрица $A' = (a'_{i,j})$ получена из матрицы A одним элементарным преобразованием строк и пусть $A'_1, \ldots, A'_m$ – столбцы A'. Предположим, что имеется линейная зависимость $\sum_{j=1}^{m} \lambda_j A_j = 0$. Это эквивалентно системе n равенств

$$(*) \qquad \sum_{j=1}^{m} \lambda_j a_{i,j} = 0, \quad i = 1, \ldots, n.$$

Пусть, например, $A \mapsto A'$ – преобразование типа (I), т.е.

$$a'_{i,j} = \begin{cases} a_{i,j} & \text{при } i \neq i_0 \\ a_{i_0,j} + \mu a_{i_1,j} & \text{при } i = i_0 \end{cases}$$

для некоторых $i_0 \neq i_1$ и μ. Тогда равенство $(*)$ сохраняется для $a'_{i,j}$ при $i \neq i_0$, а для $i = i_0$ оно дает нам

$$0 = \sum_{j=1}^{m} \lambda_j a_{i_0,j} = \sum_{j=1}^{m} \lambda_j (a'_{i_0,j} - \mu a_{i_1,j}) = \sum_{j=1}^{m} \lambda_j a'_{i_0,j} - \mu \sum_{j=1}^{m} a_{i_1,j}$$

Поскольку второй член равен нулю, то $\sum_{j=1}^{m} \lambda_j a'_{i_0,j} = 0$. Следовательно, $\sum_{j=1}^{m} \lambda_j A'_j = 0$.

Наоборот, предположим, что столбцы $A_{i_1}, \ldots, A_{i_r}$ линейно независимы. Если соответствующие столбцы $A_{i_1}, \ldots, A_{i_r}$ линейно зависимы, то из обратимости преобразования $A \mapsto A'$ мы получаем линейную зависимость столбцов $A_{i_1}, \ldots, A_{i_r}$. □

Следствие. *Ранг системы столбцов матрицы не меняется при элементарных преобразованиях строк.*

Лемма. *Пусть в матрице A минор, стоящий на пересечении строк $i_1, \ldots, i_r$ и столбцов $j_1, \ldots, j_r$, отличен от нуля. Тогда соответствующие строки (с номерами $i_1, \ldots, i_r$) линейно независимы. То же верно для столбцов (с номерами $j_1, \ldots, j_r$).*

Доказательство. Пусть M – соответствующая матрица. Согласно критерию невырожденности матрицы строки и столбцы M линейно независимы. Следовательно, линейно независимы также и удлинённые строки и столбцы. □

Лемма. *Ранг системы строк ступенчатой матрицы $A = (a_{i,j})$ равен рангу системы ее столбцов и равен числу ее ненулевых строк.*

Доказательство. Пусть $a_{1,j_1}, \ldots, a_{r,j_r}$ – лидеры строк, где $j_1 < j_2 < \cdots < j_r$ и r – числу ненулевых строк. Тогда минор, стоящий на пересечении строк $1, \ldots, r$ и столбцов $j_1, \ldots, j_r$, отличен от нуля. По предыдущей лемме ненулевые строки матрицы A линейно независимы и поэтому ранг системы строк A равен r. Далее, главные столбцы $A_{j_1}, \ldots, A_{j_r}$ также линейно независимы. Докажем, что они образуют базис системы столбцов. Пусть A_k – произвольный столбец матрицы A. Достаточно показать, что имеет место разложение $A_k = \lambda_1 A_{j_1} + \cdots + \lambda_r A_{j_r}$. Рассмотрим его как систему линейных уравнений относительно $\lambda_1, \ldots, \lambda_r$. Матрица этой системы треугольна и имеет определитель (равный минору) отличный от нуля. Следовательно, система совместна. □

Следствие. *Ранг системы строк матрицы равен рангу системы ее столбцов.*

Доказательство теоремы о ранге. Осталось доказать, что ранг матрицы не может превосходить наивысшего порядка отличного от нуля минора. Пусть в матрице строки с номерами $i_1, \ldots, i_r$ образуют базис системы строк. Докажем, что некоторый минор порядка r отличен от нуля. Пусть A' – матрица, полученная из A вычёркиванием всех строк кроме $i_1, \ldots, i_r$. Тогда $\operatorname{rk} A' = r$ (поскольку строки A' линейно независимы). Пусть теперь столбцы матрицы A' с номерами $j_1, \ldots, j_r$ образуют базис системы ее столбцов и пусть A'' – матрица, полученная из A' вычёркиванием всех столбцов, кроме $j_1, \ldots, j_r$. Снова $\operatorname{rk} A'' = r$ (поскольку столбцы A'' линейно независимы). Согласно критерию невырожденности матрицы $|A''| \neq 0$. □

Алгоритм нахождения базиса

. . . . . .

Теорема. $\operatorname{rk}(AB) \leq \operatorname{rk} A,\ \operatorname{rk} B$.

Доказательство. Пусть $C := AB$. Мы считаем, что $A = (a_{i,j})$, $B = (b_{i,j})$, $C = (c_{i,j})$ и размеры матриц A, B, C – $n \times m$, $m \times q$ и $n \times q$, соответственно. Пусть $C_1, \ldots, C_q$ – столбцы C и пусть $A_1, \ldots A_m$ – столбцы A. На i-ом месте столбца C_j стоит элемент $c_{i,j} = \sum_{k=1}^{m} a_{i,k} b_{k,j}$. Поэтому $C_j = \sum_{k=1}^{m} b_{k,j} A_k$. Таким образом, столбцы матрицы C линейно выражаются через столбцы матрицы A. По следствию из леммы о линейной зависимости имеем $\operatorname{rk} C \le \operatorname{rk} A$. Второе неравенство следует из того, что

$$\operatorname{rk} C = \operatorname{rk} C^{\mathrm{T}} = \operatorname{rk}(B^{\mathrm{T}} A^{\mathrm{T}}) \le \operatorname{rk} B^{\mathrm{T}} = \operatorname{rk} B.$$

□

. . . . . .

Критерий совместности системы линейных уравнений

Теорема (Кронекера–Капелли)**.** *Система линейных уравнений $AX = B$ совместна* $\iff \operatorname{rk} A = \operatorname{rk}(A \mid B)$.

Доказательство. $\Rightarrow$ Пусть $x_1 = \lambda_1, \ldots, x_n = \lambda_n$ – решение. Тогда $\lambda_1 A_1 + \cdots + \lambda_n A_n = B$, т.е. столбцы матрицы (A, B) выражаются через столбцы матрицы A. По лемме о линейной зависимости $\operatorname{rk} A \ge \operatorname{rk}(A \mid B)$. Очевидно также, что $\operatorname{rk} A \le \operatorname{rk}(A \mid B)$.

$\Leftarrow$ Пусть $\operatorname{rk} A = \operatorname{rk}(A \mid B) = r$. Пусть $A_{i_1}, \ldots, A_{i_r}$ базис столбцов матрицы A. Тогда это и базис столбцов матрицы $(A \mid B)$. Следовательно, B выражается через этот базис: $\lambda_{i_1} A_{i_1} + \cdots + \lambda_{i_r} A_{i_r} = B$. Полагая $\lambda_j = 0$ при $j \notin \{i_1, \ldots, i_r\}$, мы можем записать $\lambda_1 A_1 + \cdots + \lambda_n A_n = B$, т.е. $(\lambda_1, \ldots, \lambda_n)$ – решение. □

Пространство решений однородной системы линейных уравнений

Все решения системы $AX = B$ от n неизвестных образуют подпространство в $\mathbb{R}^n$ тогда и только тогда, когда $B = 0$, т.е. система однородна.

Определение. *Фундаментальной системой решений* однородной системы называется любой базис пространства решений однородной системы.

Теорема (размерность пространства решений однородной системы уравнений)**.** *Пусть $AX = 0$ – однородная система линейных уравнений, где $X = (x_1, \ldots, x_n)^{\mathrm{T}}$ и пусть V – пространство решений. Тогда*

$$\dim V = n - \operatorname{rk} A.$$

Доказательство. Пусть $r := \operatorname{rk} A$ и пусть $x_{i_1}, \ldots, x_{i_{n-r}}$ – свободные неизвестные. Все неизвестные выражаются через свободные:

$$x_j = \sum_{k=0}^{n-r} b_{j,k} x_{i_k}, \qquad j = 1, \ldots n.$$

Построим базис $\mathbf{e}_1, \ldots, \mathbf{e}_{n-r} \in V$. Например,

- $\mathbf{e}_s = (\alpha_1^s, \cdots, \alpha_n^s)$, где
$$\alpha_{i_k}^s = \delta_{k,s} = \begin{cases} 1 & \text{если } k = s, \\ 0 & \text{если } k \neq s. \end{cases}$$

Остальные α_j, $j \notin \{i_1, \ldots, i_{n-r}\}$ вычисляются по формулам выше. Тогда $\mathbf{e}_s \in V$. Векторы $\mathbf{e}_1, \ldots, \mathbf{e}_{n-r}$ линейно независимы. Действительно, укороченные векторы $\mathbf{e}'_1, \ldots, \mathbf{e}'_{n-r}$, полученные из $\mathbf{e}_1, \ldots, \mathbf{e}_{n-r}$ вычеркиванием всех координат, кроме координат с номерами $i_1, \ldots, i_{n-r}$, имеют вид $\mathbf{e}'_s = (0, \ldots, \underset{\substack{\uparrow \\ s}}{1}, \ldots, 0)$. Эти векторы линейно независимы, а поэтому линейно независимы и векторы $\mathbf{e}_1, \ldots, \mathbf{e}_{n-r}$. Пусть $\mathbf{v} = (\alpha_1, \ldots, \alpha_n)$ – любое решение. Положим $\mathbf{w} = \mathbf{v} - (\alpha_{i_1}\mathbf{e}_1 + \cdots + \alpha_{i_{n-r}}\mathbf{e}_{n-r})$. Так как V – пространство, то $\mathbf{w}$ – решение. Значение свободных неизвестных для w равны нулю. Следовательно, $\mathbf{w} = \mathbf{0}$ и $\mathbf{v} = \alpha_{i_1}\mathbf{e}_1 + \cdots + \alpha_{i_{n-r}}\mathbf{e}_{n-r}$. □

Теорема. *Пусть $V \subset \mathbb{R}^n$ – m-мерное подпространство. Существует однородная система линейных уравнений $AX = 0$ с матрицей A такая что $X \in V$ тогда и только тогда, когда $AX = 0$.*

Доказательство. Если $V = \{0\}$, то утверждение очевидно. Пусть столбцы $B_1, \ldots, B_m$ составляют базис V. Составим $n \times m$-матрицу B, в которой $B_1, \ldots, B_m$ являются столбцами. Таким образом, $\operatorname{rk} B = m$. Рассмотрим систему линейных уравнений $B^{\mathrm{T}}Y = 0$, где Y – столбец n неизвестных. Пусть $Y = F_1, \ldots, F_{n-m}$ – фундаментальная система решений и пусть F – $n \times (n-m)$-матрица, в которой $F_1, \ldots, F_{n-m}$ являются столбцами. Тогда $B^{\mathrm{T}}F = 0$ и, следовательно, $F^{\mathrm{T}}B = 0$. Полагаем $A := F^{\mathrm{T}}$. Имеем $AB = 0$ и строки A линейно независимы. Пусть $W \subset \mathbb{R}^n$ – пространство решений однородной системы $AX = 0$. Далее, $AB_i = 0$. Поэтому $AX = 0$ для любого X, являющегося линейной комбинацией B_i, т.е. для любого X, принадлежащего V. Следовательно, $V \subset W$. Так как $\dim W = \dim V = m$, то $V = W$. □

Лекция 9

Подгруппы. Подкольца. Подпространства. Морфизмы алгебраических структур(случай групп, колец, векторных пространств). Изоморфизмы. Примеры. Изоморфизм векторных пространств одной размерности. Ядро и образ гомоморфизма.

Линейные отображения векторных пространств

Определение. *Линейным отображением векторных пространств* называется отображение $f : V \to W$ такое, что

$$f(a+b) = f(a) + f(b) \qquad f(\lambda a) = \lambda f(a) \qquad \forall a,\, b \in V. \qquad \forall \lambda \in \mathbb{R}.$$

Линейное отображение $f : V \to V$ векторного пространства в себя называется *линейным оператором. Изоморфизмом векторных пространств* называется линейное отображение $f : V \to W$, у которого существует обратное.

Теорема. *Векторные пространства изоморфны тогда и только тогда, когда из размерности совпадают.*

. . . . . .

Гомоморфизмы групп

Определение. *Гомоморфизмом* групп называется отображение $f : G \to H$ группы G в группу H такое, что

$$f(a \circ b) = f(a) * f(b) \qquad \forall a,\, b \in G.$$

Предложение. *Пусть $f : G \to H$ – гомоморфизм групп. Тогда*

(1) $f(a^n) = f(a)^n$;

(2) $f(1_G) = 1_H$;

(3) $f(a^{-1}) = f(a)^{-1}$;

(4) *если у f существует обратное отображение, то оно тоже является гомоморфизмом.*

Примеры. (1) Определитель $\det : GL_n(\Bbbk) \to \Bbbk^*$ является гомоморфизмом групп.

(2) Знак подстановки $\operatorname{sgn} : S_n \to \{\pm 1\}$ является гомоморфизмом групп.

(3) Если A – абелева группа, то отображение $f(a) = a^n$ является гомоморфизмом. В абелевой аддитивной группе для любого $n \in \mathbb{Z}$ отображение $a \mapsto na$ является гомоморфизмом группы в себя.

(4) Экспонента $\exp : \mathbb{R} \to \mathbb{R}^*$, $a \mapsto e^a$ является гомоморфизмом групп.

(5) Взятие модуля $|\cdot| : \mathbb{R}^* \to \mathbb{R}_{>0}$, $z \mapsto |z|$ является гомоморфизмом групп.

(6) $\mathbb{Z} \to \mathbb{R}^*, \quad n \longmapsto a^n$.

Определение. Гомоморфизм групп $f : G \to H$ называется *изоморфизмом*, если существует обратное отображение. Изоморфизм $f : G \to G$ группы с собой называется *автоморфизмом.*

Примеры. (1) тождественное отображение $G \to G$ является автоморфизмом;

(2) $\mathbb{R}^+ \to \mathbb{R}_{>0}, \quad a \longmapsto e^a$ является изоморфизмом;

(3) если A – абелева группа, то отображение $f(a) = a^{-1}$ является автоморфизмом;

(4) $GL_n(\Bbbk) \to GL_n(\Bbbk), \qquad A \longmapsto (A^{-1})^{\mathrm{T}}$ является автоморфизмом;

(5) для любой группы G и элемента $a \in G$ отображение $f(x) = axa^{-1}$ является автоморфизмом. Он называется *внутренним* автоморфизмом.

Определение. Подмножество

$$\operatorname{Ker}(\varphi) := \{a \in G \mid \varphi(a) = 1_H\}$$

называется *ядром* гомоморфизма групп $\varphi : G \to H$.

Лемма. *Пусть $\varphi : G \to H$ – гомоморфизм групп. Тогда его ядро $\operatorname{Ker}(\varphi)$ является подгруппой в G, а его и образ $\operatorname{Im}(\varphi) = \varphi(G)$ – подгруппой в H.*

Доказательство. Проверим, например, первое:

$$a_1,\, a_2 \in \operatorname{Ker}(\varphi) \Longleftrightarrow \varphi(a_1) = \varphi(a_2) = 1 \Longrightarrow$$
$$\Longrightarrow \varphi(a_1 a_2^{-1}) = \varphi(a_1)\varphi(a_2)^{-1} = 1 \Longleftrightarrow a_1 a_2^{-1} \in \operatorname{Ker}(\varphi).$$

□

Замечание. Гомоморфизм $\varphi : G \to H$ является инъективным тогда и только тогда, когда $\operatorname{Ker}(\varphi) = \{1\}$.

Гомоморфизмы колец

Определение. *Гомоморфизмом колец* называется отображение $\varphi : R \to R_1$ такое, что $\varphi(a+b) = \varphi(a) + \varphi(b)$ и $\varphi(ab) = \varphi(a)\varphi(b)$ для любых элементов $a, b \in R$. Таким образом, гомоморфизм колец является гомоморфизмом их аддитивных групп. Как обычно в алгебре, биективный гомоморфизм называется *изоморфизмом*. Изоморфизм кольца на себя называется *автоморфизмом*. Если R и R_1 – кольца с единицами 1 и $1'$, то обычно считается, что гомоморфизм колец $\varphi : R \to R_1$ единицу переводит в единицу, т.е. $\varphi(1) = 1'$ (это свойство автоматически не выполняется).

Для любого кольца R определено умножение его элемента $a \in R$ на целое число $n \in \mathbb{Z}$:

$$n \cdot a = \begin{cases} \underbrace{a + \cdots + a}_{n} & \text{если } n > 0, \\ 0 & \text{если } n = 0, \\ \underbrace{a + \cdots + a}_{-n} & \text{если } n < 0. \end{cases}$$

Это умножение удовлетворяет свойствам

$$(n_1 + n_2) \cdot a = n_1 \cdot a + n_2 \cdot a, \qquad n \cdot (a_1 + a_2) = n \cdot a_1 + n \cdot a_2.$$

(проверьте!)

Предложение. *Пусть $f : R \to S$ – гомоморфизм колец. Тогда*

(1) $f(n \cdot a^n) = n \cdot f(a)$;

(2) $f(0_R) = 0_S$;

(3) $f(-a) = -f(a)$;

(4) *если у f существует обратное отображение, то оно тоже является гомоморфизмом.*

Примеры. (1) Если R – кольцо с единицей, то отображение

$$\mathbb{Z} \longrightarrow R, \qquad n \longmapsto n \cdot 1$$

является гомоморфизмом.

(2) Пусть A – кольцо числовых функций на некотором множестве M. Зафиксируем элемент $a \in M$. Отображение

$$\varphi : A \longrightarrow \mathbb{R}, \qquad f \longmapsto f(a).$$

Является гомоморфизмом.

Определение. Подмножество

$$\mathrm{Ker}(\varphi) := \{a \in G \mid \varphi(a) = 0\}$$

называется *ядром* гомоморфизма колец $\varphi : R \to S$.

Лемма. *Пусть $\varphi : R \to S$ – гомоморфизм колец. Тогда его ядро $\mathrm{Ker}(\varphi)$ является подкольцом в R, а его и образ $\mathrm{Im}(\varphi) = \varphi(R)$ – подкольцом в S.*

Замечание. Гомоморфизм $\varphi : R \to S$ колец является инъективным тогда и только тогда, когда $\mathrm{Ker}(\varphi) = \{0\}$.

. . . . . .

Понятие алгебры

Определение. *Алгеброй* A над полем $\Bbbk$ называется множество с тремя операциями: сложения элементов A между собой, умножения элементов A между собой и умножения элементов поля $\Bbbk$ на элементы A так, что выполнены следующие условия:

(1) A является кольцом;

(2) A является векторным пространством над $\Bbbk$;

(3) $\forall \alpha \in \Bbbk \quad \forall a, b \in A \;\; (\alpha a) \cdot b = a \cdot (\alpha b) = \alpha(a \cdot b)$.

Говорят, что алгебра A ассоциативна, коммутативна, с единицей и т. д. если таковым является соответствующее кольцо. Говорят, что (ассоциативная) алгебра A является *алгеброй с делением*, если в A имеется единица и для любого $a \in A$, $a \neq 0$ существует обратный элемент.

Примеры. (1) любое векторное пространство с нулевым умножением;

(2) $\mathbb{R}$ над $\mathbb{Q}$,

(3) $\{a + b\sqrt{2} \in \mathbb{R} \mid a, b \in \mathbb{Q}\}$ над $\mathbb{Q}$,

(4) $\{a_n\}$ – множество всех последовательностей над $\mathbb{R}$,

(5) $C[a, b]$ над $\mathbb{R}$,

(6) пространство векторов трехмерного пространства с операцией векторного умножения над $\mathbb{R}$;

(7) $\mathrm{Mat}_n(\Bbbk)$ над $\Bbbk$.

Гомоморфизмом алгебр называется отображение $f : A \to A'$ такое, что это гомоморфизм колец и $\Bbbk$-линейное отображение (т.е. . . . .). Гомоморфизм алгебр называется *изоморфизмом*, если у него имеется обратное отображение.

Лекция 10

Поля. Определение, свойства, примеры. Изоморфизм полей. Конечномерная ассоциативная алгебра без делителей нуля является телом. Поле комплексных чисел. Аксиоматическое определение, существование, единственность. Алгебраическая запись. Вещественная и мнимая части. Комплексное сопряжение.

Определение. *Полем* называется ассоциативное коммутативное кольцо $\Bbbk$ такое, что любой ненулевой элемент $\Bbbk$ обратим.

Примеры. (1) $\mathbb{Q}$, $\mathbb{R}$;

(2) $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt[3]{2}]$;

(3) $\mathbb{Q}(t)$, $\mathbb{R}(t)$.

. . . . . .

Поле комплексных чисел

Определение (аксиоматическое определение $\mathbb{C}$)**.** *Полем комплексных чисел* называется любое поле $\mathbb{C}$, которое обладает следующими свойствами:

(1) $\mathbb{C}$ содержит подполе $\mathbb{R}$ изоморфное полю действительных чисел;

(2) $\mathbb{C}$ содержит элемент i такой, что $i^2 = -1$;

(3) если существует подполе K такое, что $\mathbb{R} \subset K \subset \mathbb{C}$ и $i \in K$, то $K = \mathbb{C}$.

Теорема. *Поле комплексных чисел $\mathbb{C}$ существует и единственно с точностью до изоморфизма. Более точно, если $\mathbb{C}$ и $\mathbb{C}'$ – два поля, удовлетворяющих свойствам* (1), (2), (3)*, то существует изоморфизм $\varphi : \mathbb{C} \to \mathbb{C}'$, переводящий действительные числа $\mathbb{R} \subset \mathbb{C}$ в действительные $\mathbb{R}' \subset \mathbb{C}'$.*

Доказательство. Существование. Положим

$$\mathbb{C} = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \;\middle|\; a,\, b \in \mathbb{R} \right\} \subset \mathrm{Mat}_n(\mathbb{R}).$$

Легко видеть, что $\mathbb{C}$ – коммутативное подкольцо в $\mathrm{Mat}_n(\mathbb{R})$:

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix} = \begin{pmatrix} a+a' & b+b' \\ -(b+b') & a+a' \end{pmatrix},$$

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix} = \begin{pmatrix} aa'-bb' & ab'+a'b \\ -ab'-a'b & aa'-bb' \end{pmatrix} = \begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix} \begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

Так как

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}^{-1} = \frac{1}{a^2+b^2} \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in \mathbb{C},$$

то $\mathbb{C}$ – поле.

Теорема. *Пусть A – ассоциативная конечномерная алгебра с 1 над $\Bbbk$. Если $a \in A$ не является делителем 0 (и $a \neq 0$), то $\exists a^{-1}$.*

Доказательство. Для некоторого m элементы $1, a, \ldots, a^m$ линейно зависимы. Выберем это m минимальным. Таким образом,

$$\lambda_m \cdot a^m + \cdots \lambda_1 \cdot a + \lambda_0 \cdot 1 = 0, \quad \lambda_i \in \Bbbk.$$

Так как a не является делителем 0 и по нашему предположению $\lambda_0 \neq 0$. Полагаем

$$a^{-1} = -\frac{1}{\lambda_0}(\lambda_m \cdot a^{m-1} + \cdots \lambda_2 \cdot a + \lambda_1 \cdot 1).$$

□

Следствие. *Пусть A – ассоциативная конечномерная алгебра с 1. Если в A нет делителей нуля, то A – алгебра с делением. Если дополнительно алгебра A коммутативна, то A – поле.*

Имеется вложение полей

$$\mathbb{R} \hookrightarrow \mathbb{C}, \qquad a \longmapsto aE.$$

Ясно, что $\mathbb{C}$ является также векторным пространством над $\mathbb{R}$ с базисом E, I, где

$$I := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

и $I^2 = -E$. Наконец, любое промежуточное поле $\mathbb{R} \subset K \subset \mathbb{C}$ также векторным пространством над $\mathbb{R}$. Так как $\dim_{\mathbb{R}} \mathbb{C} = 2$, то или $K = \mathbb{R}$ или $K = \mathbb{C}$.

Единственность. Пусть $\mathbb{C}'$ – любое другое поле, удовлетворяющее свойствам (1), (2), (3). Построим изоморфизм φ между нашим полем $\mathbb{C}$, построенным выше, и $\mathbb{C}'$:

$$\varphi : \mathbb{C} \longrightarrow \mathbb{C}', \qquad \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \longmapsto a + bi.$$

Несложно проверяется, что φ – гомоморфизм колец.

Лемма. *Пусть $f : F \to R$ – гомоморфизм колец. Если F – поле и $f(F) \neq 0$, то f инъективен.*

Доказательство. Предположим, что $f(a) = f(b)$ и $a \neq b$. Положим $c := a - b$. Тогда $c \neq 0$ и $f(c) = f(a) - f(b) = 0$. Далее $f(cc^{-1}) = f(1) = f(c)f(c^{-1}) = 0$. Для любого $x \in F$ имеем $f(x) = f(x) \cdot f(1) = 0$. □

Следовательно, φ – вложение и $\varphi(\mathbb{C})$ – подполе в $\mathbb{C}'$, содержащее $\mathbb{R}' = \varphi(\mathbb{R})$ и элемент $i := \varphi(I)$, удовлетворяющий $i^2 = -1$. □

Следствие (алгебраическая запись комплексных чисел)**.** *$\mathbb{C}$ является двумерным векторным пространством над $\mathbb{R}$ и, таким образом, каждое комплексное число $z \in \mathbb{C}$ единственным образом представляется в виде $z = a + ib$, $a, b \in \mathbb{R}$.*

Отображение

$$\mathbb{C} \longrightarrow \mathbb{C}, \qquad z = a + ib \longmapsto \bar{z} := a - ib$$

называется *комплексным сопряжением*. При матричной реализации поля $\mathbb{C}$ комплексное сопряжение является транспонированием. Отсюда легко видеть, что комплексное сопряжение биективно и удовлетворяет следующим свойствам:

$$\overline{z + w} = \overline{z} + \overline{w}, \quad \overline{z \cdot w} = \overline{z} \cdot \overline{w}.$$

Таким образом, комплексное сопряжение – изоморфизм $\mathbb{C}$ на себя. В алгебре изоморфизм некоторого объекта на себя называется *автоморфизмом*. Отметим, что $z = \bar{z} \iff z \in \mathbb{R}$.

Лекция 11

Тригонометрическая форма комплексного числа. Формула Муавра. Решения уравнения $z^n = w$. Группа $\boldsymbol{\mu}_n$ корней из 1. Первообразные корни. Циклические группы. Кольца вычетов. Делители нуля и обратимые элементы. Поля $\mathbb{F}_p$. Конечное ассоциативное кольцо без делителей 0 является телом. Изоморфизм $\mathbb{Z}/n\mathbb{Z}$ и $\boldsymbol{\mu}_n$.

Модулем комплексного числа $z = a + ib$ называется неотрицательное действительное число $|z| := \sqrt{a^2 + b^2} = \sqrt{|z|}$. Пусть $|z| \neq 0$. Тогда $z/|z|$ – комплексное число, модуль которого равен 1, т.е. $z/|z| = a' + ib'$, где $a' = a/|z|$, $b' = b/|z|$, $a'^2 + b'^2 = 1$. Следовательно, $a' = \cos\varphi$, $b' = \sin\varphi$ для некоторого $\varphi \in \mathbb{R}$. Это φ (определенное по модулю 2π) называется *аргументом* z. Таким образом, каждое комплексное число $z \neq 0$ представляется в виде $z = r(\cos\varphi + i\sin\varphi)$ Это представление называется *тригонометрической* формой комплексного числа. Ясно, что $r'(\cos\varphi' + i\sin\varphi') = r(\cos\varphi + i\sin\varphi) \iff r' = r$ и $\varphi' = \varphi + 2\pi k$, $k \in \mathbb{Z}$.

Теорема. *Пусть* $z = r(\cos\varphi + i\sin\varphi)$ *и* $w = q(\cos\psi + i\sin\psi)$. *Тогда*

(1) $zw = rq(\cos(\varphi + \psi) + i\sin(\varphi + \psi))$;

(2) $z/w = rq(\cos(\varphi - \psi) + i\sin(\varphi - \psi))$.

Таким образом, $|zw| = |z||w|$, $\arg(zw) = \arg(z) + \arg(w)$, $\arg(z/w) = \arg(z) - \arg(w)$ *(если* $z \neq 0$ *и* $w \neq 0$*).*

Теорема (формула Муавра)**.** *Пусть* $z = r(\cos\varphi + i\sin\varphi)$ *и* $n \in \mathbb{Z}$. *Тогда*

$$z^n = r(\cos n\varphi + i\sin n\varphi).$$

Теорема. *Пусть* $w = q(\cos\psi + i\sin\psi) \neq 0$ *и* $n \in \mathbb{N}$. *Тогда уравнение* $z^n = w$ *имеет ровно* n *корней. Они могут быть записаны в виде*

$$z_k = r(\cos\varphi_k + i\sin\varphi_k), \quad r = \sqrt[n]{q},\ \varphi_k = \frac{\psi + 2\pi k}{n},\ k = 0, \ldots, n-1.$$

Обозначим через $\boldsymbol{\mu}_n$ множество всех корней степени n из 1.

Предложение. $\boldsymbol{\mu}_n$ *– группа.*

Определение. $z \in \boldsymbol{\mu}_n$ называется *первообра́зным* корнем степени n из 1, если он не является корнем меньшей степени из 1.

Предложение. *Для любого n первообразные корни степени n из 1 существуют. Все корни степени n из 1 являются степенями первообразного.*

. . . . . .

Циклические группы

Определение. Группа G называется *циклической*, если существует элемент $a \in G$ такой, что любой элемент $g \in G$ является степенью a, т.е. $g = a^k$, $k \in \mathbb{Z}$.

Примеры. (1) Группа $\boldsymbol{\mu}_n$ – циклическая, она порождается любым первообразным корнем из 1.

(2) $\mathbb{Z}$.

(3) Группа R^+ – не является циклической, она несчетна.

Задача. Является ли циклической группа $\mathbb{Q}^+$? Группа $\mathbb{Q}^*$? Пусть $\Bbbk$ – бесконечное поле. Докажите, что группы $\Bbbk^+$ и $\Bbbk^*$ не являются циклическими.

Кольца вычетов

Зафиксируем $n \in \mathbb{N}$. Будем говорить, что a, $b \in \mathbb{Z}$ *сравнимы по модулю n* если n делит $a - b$. Подмножество

$$\bar{a} := \{b \in \mathbb{Z} \mid b \equiv a \mod n\}$$

называется *классом вычетов* по модулю n. По определению $\bar{a} = \bar{a}' \iff a \equiv a' \mod n$. Таким образом, для любого $\bar{a}$ мы можем записать $\bar{a} = \bar{a}'$, где $0 \leq a' < n$. Множество всех классов обозначается через $\mathbb{Z}/n\mathbb{Z}$ (или $\mathbb{Z}_n$). Согласно сказанному выше, $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$.

Пример. Пусть $n = 2$. Тогда $\mathbb{Z}/2\mathbb{Z}$ состоит из двух элементов $\bar{0}$ (четные числа) и $\bar{1}$ (нечетные числа).

Определим сложение и умножение элементов $\mathbb{Z}/n\mathbb{Z}$ по правилам

$$\bar{a} + \bar{b} = \overline{a+b}, \qquad \bar{a}\bar{b} = \overline{ab}.$$

Корректность определения: пусть $\bar{a} = \bar{a}'$ и $\bar{b} = \bar{b}'$. Тогда $a' = a + nk$ и $b' = b + nl$. Отсюда

$$a' + b' = (a + nk) + (b + nl) = a + b + n(k + l), \qquad \overline{a'+b'} = \overline{a+b},$$

$$a'b' = (a + nk)(b + nl) = ab + n(k + l + nkl), \qquad \overline{a'b'} = \overline{ab}.$$

Теорема. $\mathbb{Z}/n\mathbb{Z}$ – *коммутативное ассоциативное кольцо с* 1.

. . . . . .

Предложение. *Пусть R – конечное ассоциативное кольцо с 1 и пусть $0 \neq a \in R$. Следующие условия эквивалентны:*

(1) *a является делителем нуля,*

(2) *a не является обратимым.*

Доказательство. Импликация (1) $\Longrightarrow$ (2) очевидна. Для доказательства (2) $\Longrightarrow$ (1) рассмотрим отображение $\varphi : R \to R$, $x \mapsto ax$. Если a не является делителем нули, то это отображение инъективно, а поскольку R – конечное множество, то φ сюръективно. Поэтому существует $a' \in R$ такой, что $1 = \varphi(a') = aa'$. Противоречие. □

Следствие. *Пусть R – конечное коммутативное ассоциативное кольцо с 1 без делителей нуля. Тогда R – поле.*

Предложение. *Пусть $n \in \mathbb{N}$, $a \in \mathbb{Z}$.*

(1) $\text{НОД}(n, a) \neq 1 \Longleftrightarrow \bar{a}$ *– делитель нуля в $\mathbb{Z}/n\mathbb{Z}$ (или $\bar{a} = \bar{0}$),*

(2) $\text{НОД}(n, a) = 1 \Longleftrightarrow \bar{a}$ *является обратимым в $\mathbb{Z}/n\mathbb{Z}$.*

Доказательство. Пусть $\text{НОД}(n, a) = d$, $k = a/d$ и $r = n/d$. Тогда $\bar{a}\bar{r} = \overline{ar} = \overline{kn} = \bar{0}$. Обратно, пусть $\bar{a}\bar{r} = \bar{0}$, $\bar{a} \neq \bar{0}$ и $\bar{r} \neq \bar{0}$. Тогда $ar \equiv 0 \mod n$ □

Следствие. *Следующие условия эквивалентны:*

(1) *$\mathbb{Z}/n\mathbb{Z}$ – поле;*

(2) *$\mathbb{Z}/n\mathbb{Z}$ не имеет делителей нуля;*

(3) *n – простое число.*

Поле $\mathbb{Z}/p\mathbb{Z}$ (где p – простое число обозначается через $\mathbb{F}_p$).

Лекция 12

Теорема Вилсона. Характеристика поля. Свойсва полей характеристики p. Отображение Фробениуса. Кольцо многочленов.

Следствие (теорема Вилсона). *Натуральное число p является простым тогда и только тогда, когда* $(p-1)! \equiv -1 \mod p$.

Характеристика поля

Определение. Пусть $\Bbbk$ – поле. Если $\underbrace{1+\cdots+1}_{n} \neq 0$ для любого n, то говорят, что $\Bbbk$ – поле характеристики 0. Если $\underbrace{1+\cdots+1}_{n} = 0$ для некоторого n, то характеристикой $\Bbbk$ называется минимальное n такое, что $\underbrace{1+\cdots+1}_{n} = 0$.

Примеры. (1) Поля $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ имеют характеристику 0.

(2) Поля $\mathbb{F}_p$ имеют характеристику $p > 0$.

Предложение. *Характеристика любого поля или равна* 0 *или является простым числом.*

Доказательство. Пусть n – характеристика поля $\Bbbk$. Предположим, что $n > 0$ и $n = n_1 n_2$, $n_i > 1$. Положим $\gamma := \underbrace{1+\cdots+1}_{n_1}$. Тогда

$$0 = \underbrace{1+\cdots+1}_{n} = \underbrace{\gamma+\cdots+\gamma}_{n_2} = \gamma \cdot (\underbrace{1+\cdots+1}_{n_2}).$$

Отсюда $\underbrace{1+\cdots+1}_{n_2} = 0$. Противоречие. □

Замечание. В любой аддитивной абелевой группы определено умножение ее элементов на целые числа. Для $n \in \mathbb{Z}$ и $a \in A$ положим

$$n \cdot a = \begin{cases} \underbrace{a+\cdots+a}_{n} & \text{если } n > 0, \\ 0 & \text{если } n = 0, \\ -((-n)\cdot a) & \text{если } n < 0. \end{cases}$$

Эта операция удовлетворяет стандарнтным свойствам (сравните с определением векторного пространства):

(1) $(n+m)\cdot a = n\cdot a + m\cdot a, \quad \forall a \in A, \forall n,\, m \in \mathbb{Z}$;

(2) $n\cdot(a+b) = n\cdot a + n\cdot b\ , \quad \forall a,\, b \in A, \forall n \in \mathbb{Z}$;

(3) $(nm)\cdot a = n\cdot(m\cdot a), \quad \forall a \in A, \forall n,\, m \in \mathbb{Z}$;

(4) $1\cdot a = a, \forall a \in A$ (здесь $1 \in \mathbb{Z}$).

Например, свойство (3) для $n,\, m > 0$ доказавается следующей выкладкой:

$$(nm)\cdot a = \underbrace{a+\cdots+a}_{nm} = \underbrace{\underbrace{(a+\cdots+a)}_{m}+\cdots+\underbrace{(a+\cdots+a)}_{m}}_{n} = \underbrace{m\cdot a+\cdots+m\cdot a}_{n} = n\cdot(m\cdot a).$$

Свойство (3) очевидно, если одно из чисел $n,\, m$ равно 0. Если оба числа $n,\, m$ отрицательны, то

$$(nm)\cdot a = ((-n)(-m))\cdot a = (-n)\cdot((-m)\cdot a) = -(n\cdot(-(m\cdot a))) = n\cdot(m\cdot a).$$

Случаи $nm < 0$ аналогичны. В частности, в любом коммутативном ассоциативном кольце определена операция умножения целых чисел на элементы кольца. Имеет место формула бинома Ньютона:

$$(a+b)^n = \sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k} = \sum_{k=0}^{n}\frac{n!}{k!(n-k)!}a^k b^{n-k}.$$

Предложение. *В поле $\Bbbk$ характеристики $p > 0$ для любых $\alpha, \beta \in \Bbbk$ выполнено равенство $(\alpha+\beta)^p = \alpha^p + \beta^p$.*

Рассмотрим отображение

$$\varphi : \Bbbk \longrightarrow \Bbbk, \qquad \alpha \in \alpha^p.$$

Предложение. *Пусть $\Bbbk' := \varphi(\Bbbk)$. Тогда $\varphi : \Bbbk \to \Bbbk'$ – изоморфизм. Если $\Bbbk$ – конечное поле, то $\varphi(\Bbbk) = \Bbbk$.*

Доказательство. Имеем

$$\varphi(\alpha\beta) = (\alpha\beta)^p = \alpha^p\beta^p = \varphi(\alpha)\varphi(\beta),$$

$$\varphi(\alpha+\beta) = (\alpha+\beta)^p = \alpha^p + \beta^p = \varphi(\alpha) + \varphi(\beta).$$

Так как $\varphi(\alpha) = \alpha^p = 0 \Longleftrightarrow \alpha = 0$, то отображение φ инъективно. □

Отображение φ называется *изоморфизмом Фробениуса.*

. . . . . .

Многочлены

Определение. Пусть R – коммутативное ассоциативное кольцо с 1. *Кольцом многочленов* от одной переменной над R называется коммутативное ассоциативное кольцо S, содержащее выделенный элемент $t \in S$, такое, что

(1) R содержится в S как подкольцо и $t \notin R$,

(2) любой элемент $f \in S$ *однозначно* представляется в виде

$$f = a_0 + a_1 t + \cdots + a_n t^n, \quad a_i \in R.$$

Элементы S называются *многочленами*. Выделенный элемент t называется независимой переменной.

Кольцо многочленов обозначается через $R[t]$.

Предложение. *Пусть R – коммутативное ассоциативное кольцо с 1. Кольцо многочленов $R[t]$ над R существует. Если $R[t']$ – другое кольцо многочленов над R, то существует изоморфизм*

$$\varphi : R[t] \longrightarrow R[t']$$

такой, что $\varphi(a) = a$ для всех $a \in R$ и $\varphi(t) = t'$.

Доказательство. Единственость. Положим

$$\varphi\left(\sum a_k t^k\right) = \sum a_k t'^k.$$

Существование. Рассмотрим множество Q всех последовательностей

$$f = (a_0, a_1, \dots, a_n, \dots)$$

таких, что только конечное число членов отлично от 0. На множестве определим сложение и умножение. Пусть

$$f = (a_0, a_1, \dots, a_n, \dots), \qquad g = (b_0, b_1, \dots, b_n, \dots).$$

Тогда

$$f + g = (c_0, c_1, \dots, c_n, \dots), \qquad f \cdot g = (d_0, d_1, \dots, d_n, \dots),$$

где $c_k = a_k + b_k$,

$$d_k = \sum_{i=0}^{k} a_i b_{k-i} = \sum_{i+j=k} a_i b_j.$$

Ясно, что Q является абелевой группой по сложению и умножение коммутативно. Пусть $f = f' + f''$, где

$$f' = (a'_0, a'_1, \dots, a'_n, \dots), \qquad f'' = (a''_0, a''_1, \dots, a''_n, \dots).$$

Запишем

$$f' \cdot g = (d'_0, d'_1, \dots, d'_n, \dots), \qquad f'' \cdot g = (d''_0, d''_1, \dots, d''_n, \dots).$$

Тогда

$$d_k = \sum_{i+j=k} a_i b_j = \sum_{i+j=k} (a'_i + a''_i) b_j = \sum_{i+j=k} a'_i b_j + \sum_{i+j=k} a''_i b_j = d'_k + d''_k.$$

Следовательно,

$$(f' + f'') \cdot g = f' \cdot g + f'' \cdot g.$$

Остается проверить ассоциативность умножения. Положим

$$s_k := (0, 0, , \dots, \underset{\substack{\uparrow \\ k}}{1}, \dots)$$

Таким образом, $s_0 = 1$. Тогда $s_k \cdot s_l = s_{k+l}$ и любой элемент $f \in S$ представляется в виде конечной суммы $f = \sum a_k s_k$, $a_k \in R$. Пусть $f = \sum a_k s_k$, $g = \sum b_l s_l$, $h = \sum c_m s_m$. Тогда

$$(f \cdot g) \cdot h = \Big(\Big(\sum a_k s_k\Big) \cdot \Big(\sum b_l s_l\Big)\Big) \cdot h = \Big(\sum a_k b_l s_{k+l}\Big) \cdot \Big(\sum c_m s_m\Big) = \sum a_k b_l c_m s_{k+l+m}$$

$$f \cdot (g \cdot h) = f \cdot \Big(\Big(\sum b_l s_l\Big) \cdot \Big(\sum c_m s_m\Big)\Big) = \Big(\sum a_k s_k\Big) \Big(\sum b_l c_m s_{l+m}\Big) = \sum a_k b_l c_m s_{k+l+m}$$

□

Лекция 13

Кольцо формальных степенных рядов. Степень многочлена. Делители нуля в кольце многочленов. Подстановка элемента в многочлен. Восстановление многочлена по его значениям. Функциональное равенство многочленов. Пример для конечных полей. Корни многочленов. Интерполяционная формула Лагранжа. Схема Горнера. Теорема Безу.

Определение. Кольцо формальных степенных рядов.

. . . . . .

Определение. Минимальное n такое, что $a_n \neq 0$ называется *степенью* f. Степень многочлена обозначается $\deg(f)$.

Предложение. *Если кольцо R не имеет делителей нуля, то для $f, g \in R[t]$, $f \neq 0$, $g \neq 0$ имеем* $\deg(fg) = \deg f + \deg g$.

Следствие. (1) *Если кольцо R не имеет делителей нуля, то и $R[t]$ не имеет делителей нуля.*

(2) *Пусть R не имеет делителей нуля. Элемент $f \in R[t]$ обратим* $\Longrightarrow \deg f = 0$, $f \neq 0$.

(3) *Пусть $\Bbbk$ – поле. Тогда $f \in \Bbbk[t]$ обратим* $\Longleftrightarrow \deg f = 0$, $f \neq 0$.

Задача. Пусть R – произвольное коммутативное ассоциативное кольцо с 1.

(1) Опишите делители 0 в $R[t]$. *Ответ*: $f \in R[t]$ делитель 0 $\Longleftrightarrow \exists\ a \in R \quad af = 0$.

(2) Опишите обратимые элементы. *Ответ*: $f = \sum a_i t^i \in R[t]$ обратим $\Longleftrightarrow a_0$ обратим и $\exists\ \ k \quad a_i^k = 0$, $i > 0$.

Подстановка элементов в многочлен. Зафиксируем $a \in R$. Отображение

$$L_a : R[t] \to R, \qquad f \mapsto f(a)$$

является гомоморфизмом колец. Каждому $f \in R[t]$ сопоставляется функция

$$\bar{f} : R \to R, \qquad a \mapsto f(a).$$

Пусть $\Bbbk$ – поле. Говорят, что $a \in \Bbbk$ – *корень* многочлена f, если $f(a) = 0$.

Многочлены и функции.

Теорема. *Пусть $f, g \in \Bbbk[t]$, $f \neq g$. Следующие условия эквивалентны:*

(1) $f(\alpha) = g(\alpha) \quad \forall \alpha \in \Bbbk$;

(2) *поле $\Bbbk$ конечно и все элементы поля $\Bbbk$ являются корнями многочлена $h := f - g$.*

. . . . . .

Теорема (Интерполяционная формула Лагранжа)**.** *Пусть $\alpha_1, \dots, \alpha_{n+1}$, $\beta_1, \dots, \beta_{n+1} \in \Bbbk$. Тогда существует единственный многочлен $f \in \Bbbk$ такой, что $\deg f \leq n$ и $f(\alpha_i) = \beta_i$.*

Доказательство.

$$f = \sum_{i=1}^{n+1} \frac{(t-\alpha_1)\cdots\widehat{(t-\alpha_i)}\cdots(t-\alpha_{n+1})}{(\alpha_i-\alpha_1)\cdots\widehat{(\alpha_i-\alpha_i)}\cdots(\alpha_i-\alpha_{n+1})}\beta_i.$$

□

Теорема (схема Горнера)**.** *Для многочлена $f \in \Bbbk[t]$ и элемента $\alpha \in \Bbbk$ имеет место представление $f = (t-\alpha)g + c$, где $c = f(\alpha)$.*

Доказательство. Пусть

$$f = \sum_{i=1}^{n} a_i t^i, \quad g = \sum_{k=0}^{n-1} b_k t^k, \quad (t-\alpha)g + c = \sum_{l=0}^{n} c_l t^l.$$

Приравнивая коэффициенты в $f = (t-\alpha)g + c$ при одинаковых степенях, получим

$$\begin{array}{lcl}
a_n = b_{n-1} & \Longrightarrow & b_{n-1} = a_n \\
a_{n-1} = b_{n-2} - \alpha b_{n-1} & \Longrightarrow & b_{n-2} = a_{n-1} + \alpha b_{n-1} \\
\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots & & \\
a_k = b_{k-1} - \alpha b_k & \Longrightarrow & b_k = a_k + \alpha b_{k-1} \\
\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots & & \\
a_1 = b_0 - \alpha b_1 & \Longrightarrow & b_0 = a_1 + \alpha b_1 \\
a_0 = c - \alpha b_0 & \Longrightarrow & c = a_0 + \alpha b_0
\end{array}$$

□

Следствие (Теорема Безу)**.** *Элемент $\alpha \in \Bbbk$ является корнем многочлена $f \in \Bbbk[t]$ $\Longleftrightarrow$ $f = (t-\alpha)g$ для некоторого $g \in \Bbbk[t]$.*

Следствие. *Для многочлена $f \in \Bbbk[t]$ и элемента $\alpha \in \Bbbk$ имеет место представление $f = c_n(t-\alpha)^n + \cdots + c_1(t-\alpha) + c_0$, где $c_i \in \Bbbk$.*

Лекция 14

Кратность корня. Деление многочленов над полем с остатком. Делимость в кольцах. Неприводимые многочлены. Наибольший общий делитель. Алгоритм Евклида. Факториальность кольца многочленов над полем. Факториальные и евклидовы кольца. Дифференцирования. Дифференцирования кольца многочленов над полем.

Кратность корня.

Деление многочленов над полем с остатком

Далее мы рассмотрим алгебру многочленов $\Bbbk[t]$, где $\Bbbk$ – поле.

Теорема (деление с остатком)**.** *Пусть* $\Bbbk$ *– поле. Для любых многочленов* $f, g \in \Bbbk[t]$, $g \neq 0$ *существуют единственные многочлены* $q, r \in \Bbbk[t]$ *такие, что*

$$f = gq + r, \quad \deg r < \deg g.$$

Доказательство. **Единственность.** $f = gq + r = gq' + r' \Longrightarrow g(q - q') = r - r' \Longrightarrow r = r' \Longrightarrow q = q'$.

Существование. Рассмотрим все представления $f = gq + r$. Это множество непусто: $q = 0$, $r = f$. Выберем из них то, у которого r имеет наименьшую степень. Пусть $\deg r = k \geq \deg g = m$. Запишем

$$r = c_k t^k + \cdots, \qquad g = b_m t^m + \cdots$$

Положим,

$$r_1 = r = g\frac{c_k}{b_m}t^{k-m}.$$

Тогда $\deg r_1 < \deg r$ и

$$f = g\left(q + \frac{c_k}{b_m}t^{k-m}\right) + r_1.$$

Противоречие. □

Практическое выполнение деления с остатком.

Делимость в кольцах

Определение. Ассоциативное коммутативное кольцо с 1 без делителей нуля называется *целостным* кольцом.

Пусть A – целостное кольцо. Говорят, что $f \in A$ *делится* на элемент $g \in A$, $g \neq 0$, если $f = gh$ для некоторого $h \in A$. В этом случае мы будем писать $g \mid f$ (читается "g делит f").

Предложение. (1) $f \mid g_1 \ \& \ f \mid g_2 \Longrightarrow f \mid (g_1 \pm g_2)$;

(2) $f \mid g \Longrightarrow f \mid gh, \quad \forall h \in A$;

(3) $f \mid g \ \& \ g \mid h \Longrightarrow f \mid h$;

(4) $f \mid g \ \& \ g \mid f \Longleftrightarrow f = gu$, *где* $u \in A$ – *обратимый элемент.*

Определение. Пусть R – целостное кольцо. Для f, $g \in R$ f, $g \neq 0$ определим *наибольший общий делитель* $\text{НОД}(f, g) = h$ следующим образом

- $h \mid f$, $h \mid g$;
- если $s \mid f$, $s \mid g$, то $s \mid h$.

Определение. Пусть A – целостное кольцо. Говорят, что оно *евклидово*, если существует функция $\delta : R \setminus \{0\} \to \mathbb{N} \cup \{0\}$ такая, что

(1) $a \mid b \Longrightarrow \delta(a) \leq \delta(b)$;

(2) Для любых a, $b \in A$, $b \neq 0$ существует представление $a = bq + r$, где $r = 0$ или $\delta(r) < \delta(b)$.

Для $A = \Bbbk[t]$, где $\Bbbk$ – поле положим $\delta(f) = \deg f$.

Наибольший общий делитель. Алгоритм Евклида

Теорема. *Пусть* $\Bbbk$ – *поле,* f, $g \in \Bbbk[t]$, $f \neq 0$, $g \neq 0$. *Тогда наибольший общий делитель* f *и* g *существует и единственен с точностью до пропорциональности. Более того, наибольший общий делитель* $h = \text{НОД}(f, g)$ *может быть представлен в виде* $h = fu + gv$, *где* u, $v \in \Bbbk[t]$.

Доказательство. Алгоритм Евклида

$$\begin{aligned}
f &= gq_1 + r_1 \\
g &= r_1q_2 + r_2 \\
r_1 &= r_2q_3 + r_3 \\
&\cdots\cdots\cdots\cdots\cdots\cdots \\
r_k &= r_{k+1}q_{k+2} + r_{k+2} \\
&\cdots\cdots\cdots\cdots\cdots\cdots \\
r_{n-1} &= r_nq_{n+1} + r_{n+1} \\
r_n &= r_{n+1}q_{n+2}.
\end{aligned}$$

Положим $s = r_{n+1}$ (последний ненулевой остаток).

Для доказательства последнего утверждения доказываем, что $r_k = fu_{k-1} + gu_{k-2}$ индукцией по k. □

Замечание. Наибольший общий делитель многочленов $0 \neq f, g \in \Bbbk[t]$ совпадает с многочленом $0 \neq s_1 \in \Bbbk[t]$ таким, что

- $s_1 \mid f$ и $s_1 \mid g$;
- если $0 \neq h \mid f$ и $h \mid g$, то $\deg h \leq \deg s_1$.

.

Замечание. Это разложение не единственно: $s = fu + gv = fu_1 + gv_1 \iff \frac{f}{s}(u_1 - u) + \frac{g}{s}(v_1 - v) = 0 \iff \exists r\ u_1 - u = r\frac{g}{s},\ v_1 - v = -r\frac{f}{s}$.

Замечание. Многочлены u и v в предыдущей теореме можно выбрать так, что $\deg u < \deg g$, $\deg v < \deg v$.

Доказательство. Запишем $u = gu_1 + u_0$, $v = fv_1 + v_0$. Тогда $s = fu_0 + gv_0 + fg(u_1 + v_1)$. Если $u_1 + v_1 \neq 0$, то $\deg(fu_0 + gv_0 + fg(u_1 + v_1)) > \deg f + \deg g$. □

Определение. Пусть $f \in \Bbbk[t]$, $\deg f > 0$. Говорят, что f *неприводим*, если для любого разложения $f = f_1 f_2$, $f_i \in \Bbbk[t]$ имеем $\deg f_1 = 0$ или $\deg f_2 = 0$.

Замечание. Понятие неприводимости зависит от выбора поля.

Примеры.
- $\deg f = 1$,
- $t^2 + 1 \in \mathbb{R}[t]$.

Замечание. Неприводимый многочлен f имеет корни $\iff \deg f = 1$.

Замечание. Многочлен, не имеющий корней может быть приводимым. Пример: $(t^2 + 1)^2 \in \mathbb{R}[t]$.

Замечание. Многочлен $f \in \Bbbk[t]$ степени 2 ил 3 неприводим $\iff$ имеет корней.

Разложение на множители.

. . . . . .

Факториальность кольца многочленов над полем

Теорема (факториальность кольца многочленов над полем)**.** *Пусть $f \in \Bbbk[t]$, $\deg f > 0$. Имеет место разложение: $f = f_1 \cdots f_m$, где все f_i – неприводимые многочлены. Это разложение единственно с точностью до порядка и пропорциональности.*

Доказательство. Существование. Индукция по степени.

Единственность. Индукция по степени.

Лемма. *Пусть $f \in \Bbbk[t]$ неприводим и $f \mid gh$. Тогда $f \mid g$ или $f \mid h$.*

Доказательство. Пусть $f \nmid g$. Тогда $(f, g) = 1$ и $fu + gv = 1$. Отсюда $fhu + ghv = h \Longrightarrow f \mid g$. □

Пусть $f = f_1 \cdots f_m = g_1 \cdots g_k$. □

Следствие. *Любой многочлен $f \in \Bbbk[t]$ единственным (с точностью до перестановки сомножителей) представляется в виде $f = (t - \alpha_1)^{m_1} \cdots (t - \alpha_r)^{m_r} g$, где $\alpha_1, \ldots, \alpha_r \in \Bbbk$ – все корни f, а $g \in \Bbbk[t]$ не имеет корней.*

Определение. Пусть $f \in \Bbbk[t]$, $\deg f > 0$ и пусть $\alpha \in \Bbbk$. Говорят, что α – *корень кратности* m, если $f = (t - \alpha)^m g$, где g не делится на $t - \alpha$. Говорят, что неприводимый многочлен $h \in \Bbbk[t]$ *множитель кратности* m, если $f = h^m g$, где g не делится на h.

Следствие. *Число корней многочлена $0 \neq f \in \Bbbk[t]$, подсчитанное с учетом кратностей, не превосходит его степени.*

Факториальные и евклидовы кольца

Факториальные кольца. Разложение на множители в евклидовых кольцах.

. . . . . .

Пример. Числа Эйлера $R = \mathbb{Z}[\sqrt{-3}]$, $4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$. Кольцо не является факториальным.

Дифференцирования

Пусть $\Bbbk$ – поле и пусть A – коммутативная ассоциативная алгебра над $\Bbbk$. Отображение $D : A \to A$ называется *дифференцированием* если

- D $\Bbbk$-линейно;
- $D(ab) = aD(b) + D(a)b$.

Лемма. *Пусть $D : A \to A$ – дифференцирование. Тогда*

(1) *если $1 \in A$ – единица, то $D(1) = 0$;*

(2) $D(a^n) = na^{n-1}D(a)$.

Доказательство. (1) $D(1) = D(1 \cdot 1) = 1D(1) + D(1)1 = D(1) + D(1) \Longrightarrow D(1) = 0$.

(2) Докажем по индукции: $D(a^{n+1}) = D(a^n a) = a^n D(a) + D(a^n)a = a^n D(a) + na^{n-1}D(a)a = (n + 1)a^{n+1}D(a)$. □

Теорема. *Пусть $\Bbbk$ – поле. Существует единственное дифференцирование $D : \Bbbk[t] \to \Bbbk[t]$ такое, что $D(t) = 1$.*

Доказательство. Единственность. По лемме $D(t^k) = kt^{k-1}D(t) = kt^{k-1}$. Пусть $f = \sum_k a_k t^k$. Из линейности выводим

$$D(f) = \sum_k D(a_k t^k) = \sum_k k a_k t^{k-1}.$$

Существование. Определим D формулой выше. Проверим $D(fg) = fD(g) + gD(f)$. Во-первых, проверим эту формулу для одночленов: $f = at^n$, $g = bt^m$, $D(fg) = D(abt^{n+m}) = ab(n+m)t^{n+m-1} = abnt^n t^{m-1} + abmt^m t^{n-1} = fD(g) + gD(f)$. Теперь распишем многочлены в виде суммы одночленов $f = \sum_i f_i$, $g = \sum_j g_j$, $fg = \sum_{i,j} f_i g_j$. Из линейности выводим

$$D(fg) = \sum_{i,j} D(f_i g_j)$$

$$fD(g) + gD(f) = \left(\sum_i f_i\right) \sum_j D(g_j) + \left(\sum_j g_j\right) \sum_i D(f_i) =$$

$$= \sum_{i,j} \left(f_i \sum_j D(g_j) + g_j \sum_i D(f_i) \right).$$

Соответствующие члены в этих двух суммах совпадают. □

Далее мы будем рассматривать дифференцирование $D : \Bbbk[t] \to \Bbbk[t]$, удовлетворяющее условию $D(t) = 1$. В этом случае обозначим $f' = D(f)$. Многочлен f' называется *производной* многочлена f.

Лекция 15

Дифференцирования. Понижение кратности при дифференцировании.Формула Тейлора. Основная теорема алгебры(формулировка). Сходимость последовательностей комплексных чисел. Лемма о возрастании модуля многочлена.

Теорема. *Пусть* $\Bbbk$ *– поле. Пусть* $f \in \Bbbk[t]$ *и пусть* g *– неприводимый множитель* f *кратности* m*. Предположим, что выполнено одно из следующих*

(1) $\operatorname{char}\Bbbk = 0$ *или*

(2) $\operatorname{char}\Bbbk = p > 0$, $p \nmid m$ *и* $p > \deg g$.

Тогда g *является множителем кратности* $m-1$ *для производной* f'.

Доказательство. Запишем $f = g^m h$, где $g \nmid h$. Тогда

$$f' = mg^{m-1}g'h + g^m h' = g^{m-1}(mg'h + gh').$$

Отсюда видно, что g^{m-1} делит f'. Предположим, что g^m делит f'. Тогда g делит $mg'h$. Следовательно, g делит mg'. Поскольку $\operatorname{char}\Bbbk$ равна 0 или не делит m, то $m \neq 0$ в $\Bbbk$ и поэтому g делит g'. Поскольку $\deg g' < \deg g$, мы получаем, что $g' = 0$. Запишем $g = \sum b_k t^k$. Тогда $0 = g' = \sum k b_k t^{k-1}$ т.е. $kb_k = 0 \quad \forall k$. Это возможно только если $\operatorname{char}\Bbbk = p > 0$ и $p \mid k$ как только $b_k \neq 0$. □

Следствие. *Пусть* $\Bbbk$ *– поле, характеристика которого равна* 0 *или не делит* m*. Пусть* $f \in \Bbbk[t]$ *и пусть* $\alpha \in \Bbbk$ *– корень* f *кратности* m*. Тогда* α *является корнем кратности* $m-1$ *для производной* f'.

Следствие. *Пусть* $\Bbbk$ *– любое поле. Кратные корни многочлена* $f \in \Bbbk[t]$ *– это в точности общие корни* f *и* f'.

Доказательство. Запишем $f = (t-\alpha)^m h$, где $h(\alpha) \neq 0$. Тогда

$$f' = m(t-\alpha)^{m-1}h + (t-\alpha)^m h'.$$

Если α – кратный корень f, то $m > 1$ и $f'(\alpha) = 0$. Обратно, если $f(\alpha) = f'(\alpha) = 0$, то $m \geq 1$ и $m(t-\alpha)^{m-1}h(\alpha) = 0 \Longrightarrow m(t-\alpha)^{m-1} = 0$. Следовательно, или $m = 0$ или $(t-\alpha)^{m-1} = 0$. В обоих случаях $m > 1$. □

Пример. $\operatorname{char}\Bbbk = p > 0$, $f = (t-\alpha)^p$, $f' = p(t-\alpha)^{p-1} = 0$.

Отделение кратных множителей. Пусть $f \in \Bbbk[t]$, $\operatorname{char}\Bbbk = 0$ или $> \deg f$. Вычисляем f'. По алгоритму Евклида вычисляем $h := (f, f')$. Тогда многочлен f/h имеет те же неприводимые множители, что и f, но все – с кратностью 1. В частности, многочлен f/h имеет те же корни, что и f, но все – простые.

Формула Тейлора

Теорема. *Пусть $\Bbbk$ – поле и пусть $f \in \Bbbk[t]$, $\deg f = n$. Предположим, что $\operatorname{char}\Bbbk = 0$ или $> n$. Тогда f единственным образом представляется в виде*

$$f = b_0 + b_1(t-\alpha) + b_2(t-\alpha)^2 + \cdots + b_n(t-\alpha)^n.$$

Более того, $b_k = f^{(k)}(\alpha)/k!$.

Доказательство. Имеем

$$((t-\alpha)^l)^{(k)} = \begin{cases} l(l-1)\cdots(l-k+1)(t-\alpha)^{l-k} & \text{при } k \le l \\ 0 & \text{иначе.} \end{cases}$$

Это доказывается индукцией по k. Таким образом,

$$f^{(k)} = b_k k! + (t-\alpha)\cdot(\text{многочлен}).$$

Получаем $f^{(k)}(\alpha) = b_k k!$. □

Практическое нахождение разложения при помощи схемы Горнера.

Основная теорема алгебры комплексных чисел

Определение. Поле $\Bbbk$ называется *алгебраически замкнутым*, если любой многочлен $f \in \Bbbk[t]$ положительной степени имеет по крайней мере один корень в $\Bbbk$.

Теорема. *Поле $\mathbb{C}$ алгебраически замкнуто.*

Напомним:

- $|z_1 + z_2| \le |z_1| + |z_2|$;
- $|z_1 - z_2| \ge |z_1| - |z_2|$.

Определение. $z_n \longrightarrow z_0$ если $|z_n - z_0| \longrightarrow 0$.

Лемма. $z_n \longrightarrow z_0 \iff \operatorname{Re} z_n \longrightarrow \operatorname{Re} z_0 \quad \& \quad \operatorname{Im} z_n \longrightarrow \operatorname{Im} z_0$.

Доказательство. Запишем $z_n = x_n + iy_n$, $z_0 = x_0 + iy_0$. Тогда

$$|z_n - z_0|^2 = (x_n - x_0)^2 + (y_n - y_0)^2,$$

$$|x_n - x_0| \le |z_n - z_0|, \quad |y_n - y_0| \le |z_n - z_0|.$$

□

Лемма. $z_n \longrightarrow z_0 \Longrightarrow |z_n| \longrightarrow |z_0|$.

Доказательство. $||z_n| - |z_0|| \leq |z_n - z_0|$. □

Следствие. $z_n \longrightarrow z_0 \Longrightarrow \exists c \in \mathbb{R} \quad |z_n| \leq c$.

Лемма. $z_n \longrightarrow z_0 \quad \& \quad w_n \longrightarrow w_0 \Longrightarrow z_n + w_n \longrightarrow z_0 + w_0,\ z_n w_n \longrightarrow z_0 w_0$.

Доказательство.

$$|z_n + w_n - (z_0 + w_0)| \leq |z_n - z_0| + |w_n - w_0|,$$

$$|z_n w_n - z_0 w_0| = |(z_n - z_0)w_n + (w_n - w_0)z_0| \leq$$
$$|(z_n - z_0)w_n| + |(w_n - w_0)z_0| \leq c|z_n - z_0| + |(w_n - w_0)z_0|.$$

□

Следствие. $z_n \longrightarrow z_0 \Longrightarrow \forall f \in \mathbb{C}[z] \quad f(z_n) \longrightarrow f(z_0)$.

Лемма (о возрастании модуля многочлена)**.** *Пусть* $f \in \mathbb{C}[z]$, $\deg f > 0$. *Тогда* $\forall c > 0$ $\exists R \in \mathbb{R}$ *такое, что* $|f(z)| \geq c$ *при* $|z| \geq R$.

Доказательство. Запишем

$$f(z) = a_n z^n + \cdots + a_1 z + a_0, \quad a_n \neq 0, \quad n \geq 1.$$

Пусть $A := \max |a_i|$. Тогда

$$|f(z)| = |a_n z^n + \cdots + a_1 z + a_0| =$$
$$= |z|^n \left| a_n + \frac{a_{n-1}}{z} + \cdots + \frac{a_1}{z^{n-1}} + \frac{a_0}{z^n} \right| \geq$$
$$|z|^n \left(|a_n| - \left| \frac{a_{n-1}}{z} + \cdots + \frac{a_1}{z^{n-1}} + \frac{a_0}{z^n} \right| \right) \geq$$
$$\geq |z|^n \left(|a_n| - \frac{|a_{n-1}|}{|z|} - \cdots - \frac{|a_1|}{|z|^{n-1}} - \frac{|a_0|}{|z|^n} \right)$$
$$\geq |z|^n \left(|a_n| - \frac{A}{|z|} - \cdots - \frac{A}{|z|^{n-1}} - \frac{A}{|z|^n} \right).$$

Мы можем считать, что

$$|z| \geq (nA + 1)/|a_n| > 1.$$

Тогда $|z|^k > |z|$ и

$$|f(z)| \geq |z|^n \left(|a_n| - \frac{nA}{|z|} \right) = |z|^{n-1} \left(|a_n||z| - nA \right) \geq |z|^{n-1}.$$

Таким образом, при

$$|z| \geq \max((nA + 1)/|a_n|, \ \sqrt[n-1]{c}) := R.$$

имеем $|f(z)| \geq c$. □

Лекция 16

Лемма Даламбера. Основная теорема алгебры (доказательство). Следствия. Неприводимые многочлены над $\mathbb{C}$ и $\mathbb{R}$. Поле частных целостного кольца. Поле рациональных функций.

Лемма (лемма Даламбера). *Пусть* $f \in \mathbb{C}[z]$, $\deg f > 0$, $f(z_0) \neq 0$. *Тогда* $\forall \epsilon > 0$ $\exists h \in \mathbb{C}$ *такое, что* $|h| < \epsilon$ *и* $|f(z_0 + h)| < |f(z_0)|$.

Доказательство. Запишем

$$f(z) = b_0 + b_k(z - z_0)^k + \cdots + b_n(z - z_0)^n, \quad b_k \neq 0, \quad b_n \neq 0, \quad k \geq 1.$$

Пусть w_0 – один из корней многочлена $b_0 + b_k z^k$. Будем искать h в виде $h = tw_0$, $t \in \mathbb{R}$, $0 < t < 1$. Тогда

$$f(z_0 + h) = b_0 + b_k w_0^k t^k + b_{k+1} w_0^{k+1} t^{k+1} + \cdots + b_n w_0^n t^n = \\ = b_0(1 - t^k) + \left(b_{k+1} w_0^{k+1} + \cdots + b_n w_0^n t^{n-k-1}\right) t^{k+1}$$

Пусть $C := |b_{k+1}||w_0|^{k+1} + \cdots + |b_n||w_0|^n$. При $t < |b_0|/C$ имеем

$$|f(z_0 + h)| \leq |b_0|(1 - t^k) + \left|b_{k+1} w_0^{k+1} + \cdots + b_n w_0^n t^{n-k-1}\right| \cdot t^{k+1} \leq \\ \leq |b_0|(1 - t^k) + \left(|b_{k+1}||w_0|^{k+1} + \cdots + |b_n||w_0|^n t^{n-k-1}\right) t^{k+1} \leq \\ \leq |b_0|(1 - t^k) + Ct^{k+1} = |b_0| + (Ct - |b_0|)t^k < |b_0| = |f(z_0)|.$$

Таким образом, можно взять $h = tw_0$, $0 < t < \min(|b_0|/C,\ 1)$. □

Доказательство основной теоремы алгебры. Пусть $f \in \mathbb{C}[z]$, $\deg f > 1$. Предположим, что $|f(z)| > 0, \quad \forall z \in \mathbb{C}$. Положим $M := \inf |f(z)|$. Существует последовательность $z_n \in \mathbb{C}$ такая, что $|f(z_n)| \longrightarrow M$. Имеются два случая.

Случай: последовательность $|z_n|$ *не является ограниченой.* $\forall R \quad \exists z_n \quad |z_n| > R$. Но по лемме о возрастании модуля $\forall c \quad \exists R \quad |f(z)| > c$ при $|z| > R$. Противоречие.

Случай: последовательность $|z_n|$ *ограничена.* Запишем $z_n = x_n + iy_n$. Последовательности x_n и y_n ограничены. Выберем сходящиеся подпоследовательности x_{n_k} и y_{n_k}. Последовательность $z_{n_k} = x_{n_k} + iy_{n_k}$ сходится: $z_{n_k} \longrightarrow z_0$. Тогда $f(z_{n_k}) \longrightarrow f(z_0)$. Это противоречит лемме Даламбера.

Следствие. *Неприводимые многочлены* $f \in \mathbb{C}[z]$ *– это только многочлены степени* 1.

Следствие. *Число корней многочлена $f \in \mathbb{C}[z]$, подсчитанных с учетом кратностей равно* $\deg f$.

Лемма. *Пусть $f \in \mathbb{R}[t]$. Тогда для любого $w \in \mathbb{C}$ имеем $f(\overline{w}) = \overline{f(w)}$.*

Следствие. *Пусть $f \in \mathbb{R}[t]$ и пусть $w \in \mathbb{C}$ – корень f. Тогда и $\overline{w}$ – корень f.*

Предложение. *Неприводимые многочлены $f \in \mathbb{R}[t]$ – это только многочлены степени 1 и многочлены степени 2 с отрицательным дискриминантом.*

Доказательство. Пусть $f \in \mathbb{R}[t]$ неприводим и пусть $\deg f > 1$. Тогда f не имеет действительных корней. Пусть $w \in \mathbb{C}$ – корень f. Тогда $\overline{w} \neq w$ и $\overline{w}$ – корень f. Следовательно, f делится на $(t-w)(t-\overline{w}) = t^2 - 2\operatorname{Re}(w)t + |w|^2 \in \mathbb{R}[t]$. □

Поле частных

Определение. Пусть R – целостное кольцо. Поле частных кольца R называется поле $\mathbb{K}$ такое, что

(1) $\mathbb{K}$ содержит R как подкольцо;

(2) любой элемент $f \in \mathbb{K}$ представляется в виде $f = g/h$, g, $h \in R$, $g \neq 0$.

Полем частных кольца R обозначается через $\operatorname{Frac}(R)$.

Теорема. (1) *Для любого целостного кольца R поле частных* $\operatorname{Frac}(R)$ *существует.*

(2) *Поле частных* $\operatorname{Frac}(R)$ *целостного кольца R единственно с точностью до изоморфизма, т.е. если* $\operatorname{Frac}(R)'$ *– другое поле частных, то существует изоморфизм $\varphi : \operatorname{Frac}(R) \to \operatorname{Frac}(R)'$, который является тождественным на $R \subset \operatorname{Frac}(R)$.*

Доказательство. Единственность.

. . . . . .

Существование. Рассмотрим множество

$$P := \{(a,b) \in R \times R \mid b \neq 0\}.$$

Зададим следующее отношение на этом множестве:

$$(a,b) \sim (a',b') \iff ab' = a'b.$$

Лемма. *Отношение $\sim$ является отношением эквивалентности.*

Доказательство. Ясно, что $\sim$ рефлексивно и симметрично. Докажем транзитивность. Пусть $(a,b) \sim (a',b')$ и $(a',b') \sim (a'',b'')$. Тогда $ab' = a'b$ и $a'b'' = a''b'$. Отсюда

$$ab'b'' = a'bb'' = a'b''b = a''b'b \implies ab'' = a''b \implies (a,b) \sim (a'',b'').$$

□

Обозначим через $\mathrm{Frac}(R)$ множество классов эквивалентности $P/\sim$. и определим на этом множестве операции

$$(a_1,b_1)\cdot(a_2,b_2)=(a_1a_2,b_1b_2),\quad (a_1,b_1)+(a_2,b_2)=(a_1b_2+a_2b_1,b_1b_2).$$

Лемма. *Формулы определяют корректные операции на* $\mathrm{Frac}(R)$.

Доказательство. Пусть $(a_1,b_1)\sim(a_1',b_1')$ и $(a_2,b_2)\sim(a_2',b_2')$. Тогда $a_1b_1'=a_1'b_1$ и $a_2b_2'=a_2'b_2$. Отсюда

$$(a_1b_1')(a_2b_2')=(a_1'b_1)(a_2'b_2)\implies(a_1a_2)(b_1'b_2')=(a_1'a_2')(b_1b_2)$$

и поэтому

$$(a_1,b_1)\cdot(a_2,b_2)=(a_1a_2,b_1b_2)\sim(a_1'a_2',b_1'b_2')=(a_1',b_1')\cdot(a_2',b_2').$$

Аналогично,

$$\begin{gathered}(a_1b_1')b_2b_2'+(a_2b_2')b_1b_1'=(a_1'b_1)b_2b_2'+(a_2'b_2)b_1b_1',\\ (a_1b_2+a_2b_1)b_1'b_2'=(a_1'b_2'+a_2'b_1')b_1b_2,\\ ((a_1b_2+a_2b_1),b_1b_2)\sim((a_1'b_2'+a_2'b_1'),b_1'b_2'),\\ (a_1,b_1)+(a_2,b_2)\sim(a_1',b_1')+(a_2',b_2').\end{gathered}$$

□

Класс эквивалентности пары $(a,b)\in\mathrm{Frac}(R)$ традиционно обозначается через a/b (а отношение $\sim$ в $\mathrm{Frac}(R)$ считается равенством).

Докажем, что множество $\mathrm{Frac}(R)$ с операциями $+$ и $\cdot$ является полем. При сложении приводим к общему знаменателю и все сводится к умножению числителей:

$$\frac{a}{b}+\frac{a'}{b}=\frac{ab+a'b}{b^2}=\frac{(a+a')b}{b^2}=\frac{a+a'}{b}.$$

Элемент $0/1$ является нулевым, элемент $(-a)/1$ является противоположным к $a/1$. Умножение: коммутативность и ассоциативность очевидны, элемент $1/1$ является единичным, элемент b/a является обратным к a/b. Дистрибутивность (сначала приводим к общему знаменателю):

$$\left(\frac{a_1}{b}+\frac{a_2}{b}\right)\frac{a_3}{b_3}=\frac{a_1+a_2}{b}\cdot\frac{a_3}{b_3}=\frac{(a_1+a_2)a_3}{bb_3}=\frac{a_1}{b}\cdot\frac{a_3}{b_3}+\frac{a_2}{b}\cdot\frac{a_3}{b_3}.$$

Имеется естественное вложение $R\hookrightarrow\mathrm{Frac}(R)$, $a\longmapsto a/1$. Это инъективный гомоморфизм. Мы отождествим R с подкольцом $\mathrm{Frac}(R)$. □

Примеры.
- $\mathbb{Z}\longmapsto\mathbb{Q}$;
- $\Bbbk[t]\longmapsto\Bbbk(t)$.

Пусть теперь R – факториальное кольцо. Дробь $f/g\in\mathrm{Frac}(R)$ имеет *несократимую* форму, если $\mathrm{НОД}(f,g)=1$.

Утверждение. (1) *Для любой дроби* $f/g \in \mathrm{Frac}(R)$ *имеется несократимая запись.*

(2) *Любая другая запись* $f'/g' \in \mathrm{Frac}(R)$ *этой дроби получается из несократимой* $f/g \in \mathrm{Frac}(R)$ *умножением числителя и знаменателя на некоторый ненулевой элемент* $h \in R$*:* $f' = fh$, $g' = gh$.

(3) *Несократимая форма единственна с точностью до умножения числителя и знаменателя на обратимый элемент* $h \in R$.

Доказательство. (1) сокращаем

(2) Пусть $f'/g' = f/g \Longrightarrow f'g = fg'$. Так как $(f, g) = 1$, то $f \mid f' = fh'$, $g \mid g' = gh'' \Longrightarrow fh'g = fgh'' \Longrightarrow h' = h''$.

(3) следует из (2). □

Лекция 17

Поле рациональных функций. Простейшие дроби. Многочлены над факториальным кольцом. Лемма Гаусса. Факториальность кольца многочленов над факториальным кольцом.

Поле рациональных функций.

Пусть теперь $R = \Bbbk[t]$. Тогда соответствующее поле частных $\operatorname{Quot}(R)$ называется полем рациональных функций. Говорят, что дробь $f/g \in \Bbbk(t)$ – *правильная*, если $\deg f < \deg g$.

Лемма. *Сумма правильных дробей является правильной дробью.*

Утверждение. *Любая дробь $f/g \in \Bbbk(t)$ единственным образом разлагается в сумму*

$$\frac{f}{g} = q + \frac{f^*}{g}, \qquad q \in \Bbbk[t], \quad \frac{f^*}{g} \text{ – правильная дробь.}$$

Доказательство. Делим с остатком: $f = qg + f^*$. □

Простейшие дроби

Дробь $f/g \in \Bbbk(t)$ называется *простейшей*, если $g = p^k$, где p – неприводимый многочлен и $\deg f < \deg p$.

Примеры.

- Если $\Bbbk = \mathbb{C}$, то любая простейшая дробь имеет вид $c/(t-\alpha)^k$.
- $\Bbbk = \mathbb{R}$, то любая простейшая дробь имеет вид $c/(t-\alpha)^k$ или $(at+b)/(t^2+pt+q)^k$, где t^2+pt+q не имеет действительных корней.
- Дробь $c/(t-\alpha)^k$ является простейшей над любым полем $\Bbbk$.

Теорема. *Всякая рациональная дробь f/g, где $g = p_1^{m_1} \cdots p_r^{m_r}$ – разложение в произведение неприводимых, является суммой многочлена и простейших дробей со знаменателями $p_1, \ldots, p_1^{m_1}, p_2, \ldots, p_2^{m_2}, \ldots, p_r, \ldots, p_r^{m_r}$:*

$$\frac{f}{g} = q + \sum_{i=1}^{r} \sum_{k=1}^{m_i} \frac{f_{i,k}}{p_i^k}, \qquad \deg f_{i,k} < \deg p_i.$$

Это разложение единственно с точностью до порядка.

Можно считать, что f/g – правильная дробь.

Лемма. *Пусть f/g – правильная рациональная дробь и пусть $g = g_1 g_2$ – разложение в произведение взаимно простых многочленов степеней $< \deg g$. Тогда существует разложение $f/g = f_1/g_1 + f_2/g_2$ в сумму правильных дробей. Это разложение единственно.*

Доказательство. Существуют многочлены u, v такие, что $g_1 u + g_2 v = 1$. Отсюда $f/g = fv/g_1 + fu/g_2 = f_1/g_1 + f_2/g_2 + f^*$, где f_1/g_1, f_2/g_2 – правильные дроби, а f^* – многочлен. Предположим, что $f^* \neq 0$. Тогда $\deg(gf^*) = \deg(f - f_1 g_2 - f_2 g_1) < \deg g$. Противоречие.

Пусть имеется два разложения $f/g = f_1/g_1 + f_2/g_2 = h_1/g_1 + h_2/g_2$. Тогда $(f_1 - h_1)g_2 = (h_2 - f_2)g_1$, g_1 делит $f_1 - h_1$, g_2 делит $h_2 - f_2 \Longrightarrow \deg(f_1 - h_1) \geq \deg g_1$. Противоречие. □

Следствие. *Всякая правильная рациональная дробь f/g, где $g = p_1^{m_1} \cdots p_r^{m_r}$ – разложение в произведение различных неприводимых, является суммой правильных дробей со знаменателями $p_1^{m_1}, p_2^{m_2}, \ldots, p_r^{m_r}$. Это разложение единственно с точностью до порядка.*

Доказательство. Индукция по r с использованием леммы. □

Лемма. *Всякая правильная рациональная дробь f/p^m, где p – неприводимый многочлен представляется в виде*

$$f/g = f_m/p^m + f_{m-1}/p^{m-1} + \cdots + f_1/p,$$

где $\deg f_i < \deg p$. Это разложение единственно.

Доказательство. Индукция по m. Делим f на p с остатком: $f = qp + f_m$, $\deg f_m < \deg p$, $\deg q < \deg p^{m-1} \Longrightarrow f/p^m = f_m/p^m + q/p^{m-1}$.

Единственность. Предположим, что имеется другое разложение

$$f/g = f_m^*/p^m + f_{m-1}^*/p^{m-1} + \cdots + f_1^*/p$$

и пусть $h_i = f_i - f_i^*$. Тогда

$$0 = h_m/p^m + h_{m-1}/p^{m-1} + \cdots + h_1/p,$$

Пусть h_k – первый член $\neq 0 \Longrightarrow$

$$0 = h_k + h_{k-1}p + \cdots + h_1 p^{k-1} \Longrightarrow h_k = 0.$$

□

Факториальность кольца многочленов над факториальным кольцом

Теорема. *Пусть R – факториальное кольцо. Тогда кольцо $R[t]$ факториально.*

Следствие. *Кольцо $\mathbb{Z}[t]$ факториально.*

Следствие. *Пусть $\Bbbk$ – поле. Кольцо $\Bbbk[t_1][t_2]\cdots[t_n]$ факториально.*

Пусть $\mathbb{K} := \mathrm{Frac}(R)$. Многочлен $f = a_n t^n + \cdots + a_0 \in R[t]$ называется примитивным, если $\mathrm{НОД}(a_n, \ldots, a_0) = 1$.

Лемма. *Любой многочлен $f \in \mathbb{K}[t]$ представляется в виде $f = \frac{\alpha}{\beta} f^*$, где α, $\beta \in R$, $b \neq 0$, $f^* \in R[t]$ – примитивный многочлен.*

Доказательство. Пусть $f = a_n t^n + \cdots + a_0$, где $a_i = b_i/c_i$, b_i, $c_i \in R$, $c_i \neq 0$. Положим $\beta = c_0 \cdots c_n$ и $a_i' = b_i \beta / c_i \in R$. Тогда $f = \frac{1}{\beta} \sum a_i' t^i$. Положим $\alpha = \mathrm{НОД}(a_0, \ldots, a_n)$ и $a_i^* = a_i'/\alpha$. Тогда $f = \frac{\alpha}{\beta} \sum a_i^* t^i$. □

Лемма (лемма Гаусса)**.** *Пусть f, $g \in R[t]$ – примитивные многочлены. Тогда fg – примитивный многочлен.*

Доказательство. Запишем

$$f = \sum a_i t^i, \quad g = \sum b_j t^j, \quad fg = \sum c_k t^k,$$

где

$$c_k = \sum_{i+j=k} a_i b_j.$$

Предположим противное. Тогда существует неразложимый элемент $p \in R$ такой, что

$$p \mid c_k, \quad \forall k.$$

По нашему предположению

$$\exists i \quad p \nmid a_i, \qquad \exists j \quad p \nmid b_j.$$

Выберем эти i и j минимальными. Тогда p делит все члены суммы $c_k = \sum_{i+j=k} a_i b_j$ кроме $a_i b_j$. Противоречие. □

Следствие. *Пусть f, $g \in R[t]$, причем g – примитивный многочлен. Если $g \mid f$ в кольце $\mathbb{K}[t]$, то $g \mid f$ в кольце $R[t]$.*

Доказательство. Пусть $f = gh$, где $h \in \mathbb{K}[t]$. Имеет место представление $h = \frac{\alpha}{\beta} h^*$, где $\alpha/\beta \in \mathbb{K}$ – несократимая дробь и $h^* \in R[t]$ – примитивный многочлен. Тогда $\beta f = \alpha g h^*$. Это противоречит лемме Гаусса. □

Следствие. *Пусть $f \in R[t]$ – примитивный многочлен. Тогда f – неразложимый элемент в кольце $R[t] \iff f$ неприводим в кольце $\mathbb{K}[t]$.*

Таким образом неразложимые элементы $f \in R[t]$ бывают двух типов:

- $\deg f = 0$, $f \in R$ – неразложимый элемент,

- $\deg f > 0$, f – примитивный в $R[t]$ и неприводимый в $\mathbb{K}[t]$ многочлен.

Лемма. *Пусть $p \in R[t]$ – неразложимый элемент в кольце $R[t]$ и пусть $p \mid fg$, $f, g \in R[t] \Longrightarrow p \mid f$ или $p \mid g$.*

Доказательство. Случай $\deg p = 0$. Запишем $f = af^*$, $g = bg^*$, где $f^*, g^* \in R[t]$ – примитивные многочлены, а $a, b \in R$. По лемме Гаусса f^*g^* примитивный многочлен. Поэтому $p \mid ab \Longrightarrow p \mid a$ или $p \mid b$.

Случай $\deg p > 0$. Тогда p – примитивный многочлен. Пусть $p \nmid f$ в кольце $R[t]$. Тогда $p \nmid f$ в кольце $\mathbb{K}[t]$. По соответствующей лемме для многочленов над полем имеем $p \mid g$ в кольце $\mathbb{K}[t]$. По следствию $p \mid g$ в кольце $R[t]$. □

Доказательство теоремы. Существование. Запишем $f = af^*$, где $f^* \in R[t]$ – примитивный многочлен, а $a \in R$. Индукцией по степени f^* допускает разложение в произведение неприводимых примитивных многочленов $\in R[t]$. Поскольку R факториально, то a допускает разложение в произведение неразложимых элементов.

Единственность. Пусть $f = p_1^{m_1} \cdots p_r^{m_r}$ – разложение в произведение неразложимых с наименьшим $\sum m_i$. Индукция по $\sum m_i$. Предположим, что

$$f = p_1^{m_1} \cdots p_r^{m_r} = p_1'^{k_1} \cdots p_s'^{k_s}$$

По лемме $p_1 \mid p_j'$ для некоторого j. Отсюда элементы p_1 и p_j' ассоциированы. Сокращая, получим два разложения f/p_1 с меньшим значением $\sum m_i$. По предположению индукции они совпадают. □

Лекция 18

Многочлены от нескольких переменных. Лексикографический порядок. Лемма о старшем члене.

Многочлены от нескольких переменных

Определение. Пусть R – коммутативное ассоциативное кольцо с 1. *Кольцом многочленов* от n переменных над R называется коммутативное ассоциативное кольцо S, содержащее выделенные элементы $t_1, \ldots, t_n$, такое, что

(1) R содержится в S как подкольцо и $S \neq R$,

(2) любой элемент $f \in S$ *однозначно* представляется в виде

$$f = \sum_{k_1,\ldots,k_n} a_{k_1,\ldots,k_n} t_1^{k_1} \cdots t_n^{k_n}, \quad a_{k_1,\ldots,k_n} \in R.$$

Элементы S называются *многочленами*. Выделенный элементы $t_1, \ldots, t_n$ называются независимыми переменными.

Кольцо многочленов от переменных $t_1, \ldots, t_n$ обозначается через $R[t_1, \ldots, t_n]$.

Предложение. *Пусть R – коммутативное ассоциативное кольцо с 1. Кольцо многочленов S от n переменных над R существует. Если S' – другое кольцо многочленов от n переменных над R, то существует изоморфизм*

$$\varphi : S \longrightarrow S'$$

такой, что $\varphi(a) = a$ для всех $a \in R$ и $\varphi(t_i) = t_i'$, где $t_1, \ldots, t_n$ (соотв. $t_1', \ldots, t_n'$) – независимые переменные в S (соотв., вS').

Доказательство. Единственость. Умножение в $R[t_1, \ldots, t_n]$ задается формулами

$$t_1^{k_1} \cdots t_n^{k_n} \cdot t_1^{l_1} \cdots t_n^{l_n} = t_1^{k_1+l_1} \cdots t_n^{k_n+l_n}$$

Таким образом,

$$f = \sum a_{k_1,\ldots,k_n} t_1^{k_1} \cdots t_n^{k_n}, \quad g = \sum b_{l_1,\ldots,l_n} t_1^{l_1} \cdots t_n^{l_n} \Longrightarrow$$

$$fg = \sum c_{m_1,\dots,m_n} t_1^{m_1} \cdots t_n^{m_n}, \quad c_{m_1,\dots,m_n} = \sum a_{k_1,\dots,k_n} b_{l_1,\dots,l_n},$$

где суммирование ведётся по всем наборам $k_1, \dots, k_n$, $l_1, \dots, l_n$ таким, что $k_1 + l_1 = m_1$, $\dots$, $k_n + l_n = m_n$. Рассмотрим отображение

$$\varphi : R[t_1, \dots, t_n] \longrightarrow R[t'_1, \dots, t'_n],$$

$$\varphi : \sum_{k_1,\dots,k_n} a_{k_1,\dots,k_n} t_1^{k_1} \cdots t_n^{k_n} \longmapsto \sum_{k_1,\dots,k_n} a_{k_1,\dots,k_n} t_1'^{k_1} \cdots t_n'^{k_n}.$$

Оно является изоморфизмом.

Существование. Определим $R[t_1, \dots, t_n]$ по индукции:

$$R[t_1, \dots, t_n] = R[t_1][t_2] \dots [t_n].$$

Тогда $R[t_1, \dots, t_n]$ – коммутативное ассоциативное кольцо с 1. Более того, $R[t_1, \dots, t_n]$ содержит R.

Лемма. *Любой элемент $f \in R[t_1, \dots, t_n]$ однозначно записывается в виде*

$$f = \sum_{k_1,\dots,k_n} a_{k_1,\dots,k_n} t_1^{k_1} \cdots t_n^{k_n}, \quad a_{k_1,\dots,k_n} \in R.$$

Доказательство. Индукция по n. $f \in R[t_1, \dots, t_n] = R[t_1, \dots, t_{n-1}][t_n] \Longrightarrow f = \sum_{k_n} f_{k_n} t^{k_n}$, $f_{k_n} \in R[t_1, \dots, t_{n-1}]$. По предположению индукции $f_{k_n} = \sum a_{k_1,\dots,k_{n-1},k_n} t_1^{k_1} \cdots t_{n-1}^{k_{n-1}}$. $\Longrightarrow$

$$f = \sum_{k_n} \left(\sum_{k_1,\dots,k_{n-1}} a_{k_1,\dots,k_{n-1},k_n} t_1^{k_1} \cdots t_{n-1}^{k_{n-1}} \right) t^{k_n} = \sum_{k_1,\dots,k_n} a_{k_1,\dots,k_n} t_1^{k_1} \cdots t_n^{k_n}$$

□

□

Следствие. $R[t_1, \dots, t_n] \simeq R[t_1][t_2] \dots [t_n]$.

Следствие. $R[t_1, \dots, t_n]$ *не имеет делителей* $0 \iff R$ *не имеет делителей* 0.

Следствие. $R[t_1, \dots, t_n] \simeq R[t_{\sigma(1)}, \dots, t_{\sigma(n)}], \quad \forall \sigma \in S_n$.

Определение. Многочлен

$$f = \sum_{k_1,\dots,k_n} a_{k_1,\dots,k_n} t_1^{k_1} \cdots t_n^{k_n}$$

называется *однородным* степени d, если $a_{k_1,\dots,k_n} \neq 0 \Longrightarrow \sum k_i = d$.

Разложение с сумму однородных компонент. Произведение однородных многочленов.

. . . . . .

Предложение. *Если в R нет делителей* 0, *то* $\deg(fg) = \deg f + \deg g$.

Доказательство. Рассмотрим разложение в сумму однородных компонент

$$f = f_0 + \cdots f_d, \qquad g = g_0 + \cdots g_e.$$

Тогда разложение $fg = \sum_{i,j} f_i g_j$ в сумму однородных компонент будет

$$fg = \sum h_k, \qquad h_k = \sum_{i+j=k} f_i g_j$$

(группируем однородные компоненты степени k). Компонента максимальной степени: $f_d g_e \neq 0$ поскольку в R нет делителей 0. □

Предложение. *Если в R нет делителей 0, то* $\deg_{x_k}(fg) = \deg_{x_k} f + \deg_{x_k} g$.

. . . . . .

Лексикографический порядок: $(k_1, \ldots, k_n) \prec (l_1, \ldots, l_n) \iff \exists i\colon \quad k_1 = l_1, \ \ldots, \ k_i = l_i, \ k_{i+1} < l_{i+1}$.

Для одночленов пишем $at_1^{k_1} \cdots t_n^{k_n} \prec bt_1^{l_1} \cdots t_n^{l_n}$ если $(k_1, \ldots, k_n) \prec (l_1, \ldots, l_n)$.

Лемма. *Для одночленов имеем:*

(1) $u \succ v$, $v \succ w \Longrightarrow u \succ w$;

(2) $u \succ v \Longrightarrow uw \succ vw$;

(3) $u \succ v$, $u' \succ v' \Longrightarrow uu' \succ vv'$.

Доказательство. (1) Запишем $u = at_1^{k_1} \cdots t_n^{k_n}$, $v = bt_1^{l_1} \cdots t_n^{l_n}$, $w = ct_1^{m_1} \cdots t_n^{m_n}$. Пусть i – максимальное такое, что $k_1 = l_1 = m_1, \ldots, k_{i-1} = l_{i-1} = m_{i-1}$ (т.е. t_i – первая переменная, входящая в u, v, w в различных степенях). $\Longrightarrow k_i \geq l_i \geq m_i$. Причем по крайней мере одно из этих неравенств – строгое.

(2) Запишем $u = at_1^{k_1} \cdots t_n^{k_n}$, $v = bt_1^{l_1} \cdots t_n^{l_n}$, $w = ct_1^{m_1} \cdots t_n^{m_n}$. Пусть i – максимальное такое, что $k_1 = l_1, \ \ldots, \ k_{i-1} = l_{i-1}$. $\Longrightarrow k_i > l_i \Longrightarrow k_1 + m_1 = l_1 + m_1, \ \ldots, \ k_{i-1} + m_{i-1} = l_{i-1} + m_{i-1}, \ k_i + m_i > l_i + m_i$.

(3) $uu' \succ vu' \succ vv'$. □

Старший член многочлена $f \in R[t_1, \ldots, t_n]$: $at_1^{k_1} \cdots t_n^{k_n} \in f$ – старший если $at_1^{k_1} \cdots t_n^{k_n} \prec bt_1^{l_1} \cdots t_n^{l_n}$ для любого другого $bt_1^{l_1} \cdots t_n^{l_n} \in f$.

Введем временное обозначение $c(f)$ – старший член f, $o(f) = f - c(f)$

Пример. $f = t_1^2 t_2 + t_1 t_2 + t_1 t_2^2 + t_3^5 \Longrightarrow t_1^2 t_2$ – старший член.

Предложение. $c(fg) = c(f)c(g)$ *(старший член произведения равен произведению старших членов).*

Доказательство. Пусть $\tilde{f} \in o(f)$, $\tilde{g} \in o(g)$. Тогда $c(f) \succ \tilde{f}$, $c(g) \succ \tilde{g} \Longrightarrow c(f)c(g) \succ \tilde{f}\tilde{g}$, $c(f)c(g) \succ c(f)\tilde{g}$, $c(f)c(g) \succ \tilde{f}c(g) \Longrightarrow c(f)c(g)$ – старший член. □

Лекция 19

Симметрические многочлены. Основная теорема и симметрических многочленах. Формулы Виета. Дискриминант. Результант (определение и свойства).

Симметрические многочлены

Пусть R – комутативное ассоциативное кольцо с 1. Пусть $f \in R[t_1, \ldots, t_n]$ и пусть $\delta \in S_n$ – подстановка. Определим новый многочлен

$$f^\delta(t_1, \ldots, t_n) := f(t_{\delta(1)}, \ldots, t_{\delta(n)}).$$

Таким образом, если $f = \sum_{k_1,\ldots,k_n} a_{k_1,\ldots,k_n} t_1^{k_1} \cdots t_n^{k_n}$, то

$$f^\delta = \sum_{k_1,\ldots,k_n} a_{k_1,\ldots,k_n} t_{\delta(1)}^{k_1} \cdots t_{\delta(n)}^{k_n}.$$

Например, если $\delta = [1, 2, 3]$ и $f = t_1 + t_2^2 + t_3^3 + t_4^4$, то $f^\delta = t_2 + t_3^2 + t_1^3 + t_4^4$.

Определение. Многочлен называется *симметрическим*, если $f^\delta = f, \quad \forall \delta \in S_n$.

Поскольку S_n порождается транспозициями, то равенство $f^\delta = f$ достаточно проверить для транспозиций.

Пример.

- Все многочлены от одной переменной – симметрические.
- *Степенные суммы* $s_m := t_1^m + \cdots + t_n^m$.
- *Элементарные симметрические многочлены*

$$\sigma_m := \sum_{i_1 < \cdots < i_m} t_{i_1} \cdots t_{i_m} \quad 1 \le m \le n.$$

Таким образом,

$$\sigma_1 = \sum x_i, \quad \sigma_2 = \sum_{i<j} x_i x_j, \quad \ldots, \quad \sigma_n = \prod x_i.$$

- *Определитель Вандермонда*

$$\Delta := \begin{vmatrix} 1 & t_1 & \cdots & t_1^{n-1} \\ 1 & t_2 & \cdots & t_2^{n-1} \\ \cdots & \cdots & \cdots & \cdots \\ 1 & t_n & \cdots & t_n^{n-1} \end{vmatrix} = \prod_{i>j}(t_i - t_j)$$

Меняет знак при транспозициях. Поэтому Δ^2 – симметрический многочлен.

Формулы Виета.

Теорема. *Пусть* $f = \sum_{k=0}^{n} a_k t^k \in \Bbbk[t]$, $\deg f = n > 0$ *и пусть* $\alpha_1, \ldots, \alpha_n$ *– корни многочлена, перечисленные с учетом кратностей. Тогда*

$$\begin{array}{ll} -a_{n-1}/a_n & = \alpha_1 + \cdots + \alpha_n \\ a_{n-2}/a_n & = \alpha_1\alpha_2 + \cdots + \alpha_{n-1}\alpha_n \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots & \\ (-1)^{n-1}a_1/a_n & = \hat{\alpha}_1 \cdots \alpha_n + \cdots + \alpha_1 \cdots \hat{\alpha}_n \\ (-1)^n a_0/a_n & = \alpha_1 \cdots \alpha_n \end{array}$$

Предложение. *Все симметрические многочлены образуют подкольцо*

$$R[t_1, \ldots, t_n]^{S_n} \subset R[t_1, \ldots, t_n].$$

Теорема (основная теорема о симметрических многочленах)**.** *Любой симметрический многочлен единственным образом представляется в виде многочлена от элементарных симметрических.*

Обозначение: $t_1^{k_1} \cdots t_n^{k_n} \in f$ если $at_1^{k_1} \cdots t_n^{k_n}$ присутствует в $f \in R[t_1, \ldots, t_n]$ с ненулевым коэффициентом a.

Лемма. *Пусть* $f \in R[t_1, \ldots, t_n]^{S_n}$ *и пусть* $u = at_1^{k_1} \cdots t_n^{k_n} = c(f)$. *Тогда* $k_1 \geq \cdots \geq k_n$.

Доказательство. Предположим, что $k_i < k_{i+1}$. Возьмем это i минимальным. Рассмотрим $\delta = [i, i+1] \in S_n$. Тогда $u = at_1^{k_1} \cdots t_i^{k_i} t_{i+1}^{k_{i+1}} \cdots t_n^{k_n} \in f \Longrightarrow u^\delta = at_1^{k_1} \cdots t_{i+1}^{k_{i+1}} t_i^{k_i} \cdots t_n^{k_n} \in f$. Но $u^\delta \succ u$. Противоречие. □

Лемма. *Для любого одночлена* $u = t_1^{k_1} \cdots t_n^{k_n}$ *такого, что* $k_1 \geq \cdots \geq k_n$ $\exists!$ $(l_1, \ldots, l_n)$ *такой, что* $c(\sigma_1^{l_1} \cdots \sigma_n^{l_n}) = u$.

Доказательство. $c(\sigma_r) = t_1 \cdots t_r \Longrightarrow$

$$c(\sigma_1^{l_1} \cdots \sigma_n^{l_n}) = t_1^{l_1}(t_1t_2)^{l_2} \cdots (t_1 \cdots t_n)^{l_n} = t_1^{l_1+\cdots+l_n} t_2^{l_2+\cdots+l_n} \cdots t_n^{l_n}.$$

Решаем систему

$$\begin{cases} l_1 + \cdots + l_n = k_1 \\ l_2 + \cdots + l_n = k_2 \\ \cdots\cdots\cdots\cdots \\ l_n = k_n \end{cases}$$

Получаем единственное решение

$$l_n = k_n, \qquad l_i = k_i - k_{i+1}, \quad i < n.$$

□

Доказательство теоремы. Существование. Предположим противное. Пусть M – множество всех $f \in R[t_1, \dots, t_n]^{S_n}$, для которых теорема не верна. Выберем $f \in M$ с наименьшим $c(f)$. По лемме $\exists\ \sigma_1^{l_1} \cdots \sigma_n^{l_n}$ такой, что $\alpha c(\sigma_1^{l_1} \cdots \sigma_n^{l_n}) = c(f)$. Тогда для $f_1 = f - \alpha c(\sigma_1^{l_1} \cdots \sigma_n^{l_n})$ имеем $c(f_1) \prec c(f)$. Противоречие.

Единственность. Пусть $g_1(\sigma_1, \dots, \sigma_n) = g_2(\sigma_1, \dots, \sigma_n)$. Положим $h = g_1 - g_2$. Разложим h в сумму одночленов

$$h = \sum h_i.$$

Ясно, что $h_i(\sigma_1, \dots, \sigma_n) \neq 0$. Пусть $u_i := c(h_i(\sigma_1, \dots, \sigma_n))$. По последней лемме среди u_i нет пропорциональных. Пусть u_* – старший среди них. Тогда u_* – старший среди всех одночленов в $h(\sigma_1, \dots, \sigma_n)$ и он не может сократиться. □

Практическая реализация. Пусть $f \in R[t_1, \dots, t_n]^{S_n}$. Можно считать, что f однороден степени d. Пусть $c(f) = at_1^{k_1} \cdots t_n^{k_n}$, $\sum k_i = d$. Выберем все наборы $(r_1, \dots, r_n)$ неотрицательных целых чисел такие, что

- $r_1 \geq \cdots \geq r_n$;
- $\sum r_i = d$;
- $(r_1, \dots, r_n) \prec (k_1, \dots, k_n)$.

Тогда $g(\sigma_1, \dots, \sigma_n)$ содержит все одночлены вида

$$\sigma_1^{r_1 - r_2} \cdot \sigma_2^{r_2 - r_1} \cdots \sigma_{n-1}^{r_{n-1} - r_n} \cdot \sigma_n^{r_n}.$$

Их коэффициенты находятся методом неопределённых коэффициентов.

Следствие. *Пусть $\Bbbk$ – поле. Пусть $f \in \Bbbk[t]$, $f = a_n t^n + \cdots a_1 t + a_0$ и пусть $\alpha_1, \dots, \alpha_n$ – корни, выписанные с учетом кратностей. Любой симметрический многочлен $\alpha_1, \dots, \alpha_n$ выражается в виде многочлена от $a_0/a_n, \dots, a_{n-1}/a_n$.*

Дискриминант

Пусть $\Bbbk$ – поле. Пусть $f \in \Bbbk[t]$, $f = a_n t^n + \cdots a_1 t + a_0$ и пусть $\alpha_1, \dots, \alpha_n$ – корни, выписанные с учетом кратностей. Определим дискриминант многочлена f следующим образом

$$D = a_n^{2n-2} \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

Дискриминант выражается через определитель Вандермонда:

$$D = a_n^{2n-2} \begin{vmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \end{vmatrix}^2$$

Предложение. *D выражается как многочлен с целыми коэффициентами от a_i.*

Доказательство. D является многочленом (с целыми коэффициентами) от элементарных симметрических функций $\sigma_i(\alpha_1, \dots, \alpha_n)$:

$$D = a_n^{2n-2} \cdot h(\sigma_1, \dots, \sigma_n).$$

По формулам Виета

$$\sigma_1 = -a_{n-1}/a_n, \quad \sigma_2 = a_{n-2}/a_n, \ \dots, \ \sigma_n = (-1)^n a_0/a_n.$$

Знаменатель каждого одночлена $\sigma_1^{l_1}\sigma_2^{l_2}\cdots\sigma_n^{l_n}$ в h равен $a_n^{l_1+\cdots+l_n}$. С другой стороны,

$$c(\sigma_1^{l_1}\sigma_2^{l_2}\cdots\sigma_n^{l_n}) = \alpha_1^{l_1+\cdots+l_n}\alpha_2^{l_2+\cdots+l_n}\cdots\alpha_n^{l_n} \quad \Longrightarrow$$

$$\sum l_i = \deg_{\alpha_1}(\sigma_1^{l_1}\sigma_2^{l_2}\cdots\sigma_n^{l_n}) \le 2n-2.$$

(из определителя Вандермонда). Таким образом, знаменатель $a_n^{2n-2}\sigma_1^{l_1}\sigma_2^{l_2}\cdots\sigma_n^{l_n}$ – многочлен от $a_0, \dots a_n$ с целыми коэффициентами. □

Пример. Пусть $n = 2$. Тогда $f = a_0 + a_1 t + a_2 t^2$,

$$D = a_2^2(\alpha_2 - \alpha_1)^2 = a_2^2(\alpha_1 + \alpha_2)^2 - 4a_2^2\alpha_1\alpha_2 = a_1^2 - 4a_0a_2.$$

Пример. Пусть $f = t^3 + pt + q$. Тогда $D = -4p^3 - 27q^2$.

Формулы Кардано Найдем корни многочлена $f = t^3 + pt + q$. Положим $t = u + v \Longrightarrow$

$$u^3 + v^3 + (u+v)(3uv + p) + q = 0.$$

Потребуем $3uv + p = 0$. Тогда

$$\begin{cases} u^3 + v^3 = -q \\ uv = -p/3 \end{cases} \Longrightarrow \begin{cases} u^3 + v^3 = -q \\ u^3v^3 = -p^3/27 \end{cases}$$

u^3 и v^3 находятся из решения $x^2 + qx - p^3/27 = 0$. Таким образом,

$$u^3,\, v^3 = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} = -\frac{q}{2} \pm \sqrt{-D}.$$

Задача. Какой смысл имеет знак дискриминанта для кубического многочлена $f \in \mathbb{R}[t]$?

Результант

Пусть $\Bbbk$ – поле. Пусть $f,\, g \in \Bbbk[t]$,

$$f = a_n t^n + \cdots a_1 t + a_0, \quad g = b_m t^m + \cdots b_1 t + b_0$$

и пусть $\alpha_1, \dots, \alpha_n$, $\beta_1, \dots, \beta_m$ – корни, выписанные с учетом кратностей. Положим

$$R(f, g) := a_n^m b_m^n \prod_{i,j} (\alpha_i - \beta_j).$$

Предложение.

- $R(f,g) = (-1)^{nm} R(g,f)$;
- $R(f,g) = a_n^m \prod_i g(\alpha_i), \quad R(g,f) = b_m^n \prod_j f(\beta_j)$;
- *(основное свойство)* $R(f,g) = 0 \iff f$ *и* g *имеют общий корень (или* $a_n b_m = 0$*).*

Доказательство. Заметим, что $g(\alpha_i) = b_m \prod(\alpha_i - \beta_j)$, $f(\beta_j) = a_n \prod(\beta_j - \alpha_i)$. □

Теорема. $R(f,f') = (-1)^{n(n-1)/2} a_n D$.

Доказательство. Имеем $R(f,f') = a_n^{n-1} \prod_i f'(\alpha_i)$.

$$f = a_n \prod_j (t - \alpha_j) \Longrightarrow f' = a_n \sum_{k=1}^{n} \prod_{j \neq k} (t - \alpha_j) \Longrightarrow$$

$$f'(\alpha_i) = a_n \prod_{j \neq i} (\alpha_i - \alpha_j) \Longrightarrow$$

$$R(f,f') = a_n^{n-1} a_n^n \prod_i \prod_{j \neq i} (\alpha_i - \alpha_j) = (-1)^{n(n-1)/2} a_n \; a_n^{2n-2} \prod_{j>i} (\alpha_i - \alpha_j)^2.$$

□

Лекция 20

Вычисление результанта. Циклические группы. Примеры. Подгруппа циклической группы. Циклические подгруппы. Порядок элемента.

Вычисление результанта

Теорема.

$$R(f,g) = \begin{vmatrix} a_n & a_{n-1} & \dots & a_0 & & & & \\ & a_n & a_{n-1} & \dots & a_0 & & & \\ & & \dots & \dots & \dots & \dots & \dots & \\ & & & & a_n & a_{n-1} & \dots & a_0 \\ b_m & b_{m-1} & \dots & \dots & b_0 & & & \\ & b_m & b_{m-1} & \dots & \dots & b_0 & & \\ & & & \dots & \dots & \dots & & \\ & & & & b_m & b_{m-1} & \dots & b_0 \end{vmatrix}$$

(Определитель порядка $n+m$. Пустые места заполняются нулями.)

Доказательство. Обозначим матрицу в правой части через A. Положим $N := n+m$. Рассмотрим вспомогательный определитель

$$|B| = \begin{vmatrix} \beta_1^{N-1} & \beta_2^{N-1} & \cdots & \beta_m^{N-1} & \alpha_1^{N-1} & \alpha_2^{N-1} & \cdots & \alpha_n^{N-1} \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ \beta_1^2 & \beta_2^2 & \cdots & \beta_m^2 & \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \beta_1 & \beta_2 & \cdots & \beta_m & \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ 1 & 1 & \cdots & 1 & 1 & 1 & \cdots & 1 \end{vmatrix}$$

Вычислим $a_n^m b_m^n |A||B|$ двумя способами.
Первое вычисление: B отличается от определителя Вандермонда только перестановками строк $\Longrightarrow$

$$|B| = \prod_{i<j}(\beta_i - \beta_j) \prod_{i,j}(\beta_j - \alpha_i) \prod_{i<j}(\alpha_i - \alpha_j)$$

Отсюда

$$a_n^m b_m^n |A||B| = |A| R(g,f) \prod_{i<j}(\beta_i - \beta_j) \prod_{i<j}(\alpha_i - \alpha_j)$$

Второе вычисление:

$$C := AB = \left(\begin{array}{c|c} I & II \\ \hline III & IV \end{array}\right) = (c_{i,j})$$

(I)
$$c_{i,j} = a_n\beta_j^{N-i} + a_{n-1}\beta_j^{N-i-1} + \cdots + a_0\beta_j^{m-i} = \beta_j^{m-i}f(\beta_j).$$

(II)
$$c_{i,m+j} = a_n\alpha_j^{N-i} + a_{n-1}\alpha_j^{N-i-1} + \cdots + a_0\alpha_j^{m-i} = \alpha_j^{m-i}f(\alpha_j) = 0.$$

(III)
$$c_{m+i,j} = b_m\beta_j^{N-i} + b_{m-1}\beta_j^{N-i-1} + \cdots + b_0\beta_j^{n-i} = \beta_j^{n-i}g(\beta_j) = 0.$$

(IV)
$$c_{m+i,m+j} = b_m\alpha_j^{N-i} + b_{m-1}\alpha_j^{N-i-1} + \cdots + b_0\alpha_j^{n-i} = \alpha_j^{n-i}g(\alpha_j).$$

Таким образом,

$$|A||B| = \left|\begin{array}{c|c} * & 0 \\ \hline 0 & ** \end{array}\right|, \quad * = \beta_j^{m-i}f(\beta_j),\ ** = \alpha_j^{n-i}g(\alpha_j).$$

$$|A||B| = \prod_j f(\beta_j)\prod_j g(\alpha_j)\begin{vmatrix} \beta_1^{m-1} & \beta_2^{m-1} & \cdots & \beta_m^{m-1} \\ \vdots & \vdots & \cdots & \vdots \\ \beta_1^2 & \beta_2^2 & \cdots & \beta_m^2 \\ \beta_1 & \beta_2 & \cdots & \beta_m \\ 1 & 1 & \cdots & 1 \end{vmatrix}\begin{vmatrix} \alpha_1^{n-1} & \cdots & \alpha_n^{n-1} \\ \vdots & \cdots & \vdots \\ \alpha_1^2 & \cdots & \alpha_n^2 \\ \alpha_1 & \cdots & \alpha_n \\ 1 & \cdots & 1 \end{vmatrix}$$

$$|A||B| = \prod_j f(\beta_j)\prod_j g(\alpha_j)\prod_{i<j}(\beta_i - \beta_j)\prod_{i<j}(\alpha_i - \alpha_j)$$

Отсюда

$$a_n^m b_m^n|A||B| = R(f,g)R(g,f)\prod_{i<j}(\beta_i - \beta_j)\prod_{i<j}(\alpha_i - \alpha_j)$$

Сравнивая с первым вычислением, получим $|A| = R(f,g)$. □

Приложения: исключения неизвестных.

. . . . . .

Определение. Квадратная матрица A называется *ортогональной*, если $AA^{\mathrm{T}} = E$.

Примеры. (1) Множество всех ортогональных $n \times n$-матриц является группой и обозначается через $O_n(\Bbbk)$ (ортогональная группа).

(2) Множество всех ортогональных $n \times n$-матриц с определителем 1 является группой и обозначается через $SO_n(\Bbbk)$ (специальная ортогональная группа).

Циклические группы

Определение. Пусть G – группа и пусть $S \subset G$ – подмножество. Положим

$$\langle S \rangle := \{a_1^{n_1} \cdots a_m^{n_m} \mid a_i \in S, \quad n_i \in \mathbb{Z}\}.$$

Ясно, что $\langle S \rangle$ – подгруппа в G. Говорят, что группа G *порождается* множеством S, если $\langle S \rangle = G$. Иначе говоря, любой элемент $g \in G$ представляется в виде произведения степеней элементов из S.

Замечание. $\langle S \rangle$ – наименьшая подгруппа в G, содержащая S.

Примеры. (1) Симметрическая группа S_n порождается транспозициями.

(2) Полная линейная группа $GL_n(\Bbbk)$ порождается элементарными матрицами.

(3) $\mathbb{Q}^*$ порождается простыми числами.

(4) $\Bbbk(t)^+$ порождается $\Bbbk[t]$ и простейшими дробями.

(5) $\Bbbk(t)^*$ порождается неприводимыми многочленами и $\Bbbk^*$.

Замечание. Не всякая группа порождается конечным числом элементов. Например, группа $\mathbb{R}^+$ несчётна, поэтому не может порождаться конечным числом элементов.

Задача. Докажите, что группы $\mathbb{Q}^+$ и $\mathbb{Q}^*$ не могут быть порождены конечным числом элементов.

Задача. Является ли конечно порожденной группа $\mathbb{Q}/\mathbb{Z}$?

Определение. Группа называется *циклической*, если она порождается одним элементом.

Примеры. (1) Группа $\boldsymbol{\mu}_n$ – циклическая, она порождается любым первообразным корнем из 1.

(2) $\mathbb{Z}/n\mathbb{Z}$.

(3) $\mathbb{Z}$.

(4) Группа R^+ – нециклическая, она несчетна.

Задача. Является ли циклической группа $\mathbb{Q}^+$? Группа $\mathbb{Q}^*$? Пусть $\Bbbk$ – бесконечное поле. Докажите, что группы $\Bbbk^+$ и $\Bbbk^*$ не являются циклическими.

В любой группе G любой элемент $a \in G$ порождает циклическую подгруппу $\langle a \rangle$. Более того, $G = \cup_{a \in G} \langle a \rangle$. Назовем *порядком элемента* $a \in G$

$$|a| = \begin{cases} \min k \in \mathbb{N} : a^k = 1 & \text{если } \exists\ k\ a^k = 1; \\ \infty & \text{если } a^k \neq 1\ \forall k. \end{cases}$$

Назовем *порядком группы* число ее элементов. Обозначение: $|G|$.

В конечной группе порядок любого элемента конечен.

Замечание. (1) $|a| = \infty \Longrightarrow$ все элементы a_k, $k \in \mathbb{Z}$ различны.

(2) $|\langle a \rangle| = |a|$.

(3) $|a| = n < \infty \Longrightarrow \langle a \rangle = \{1, a, \ldots, a^{n-1}\}$. Конечная группа является циклической $\Longleftrightarrow \exists a \in G \ |a| = |G|$.

(4) $|a| = n < \infty \Longrightarrow$

(a) $a^m = 1 \Longleftrightarrow n \mid m$;

(b) $a^k = a^l \Longleftrightarrow k \equiv l \mod n$.

Примеры. (1) Элементы конечного порядка в $\Bbbk^+$.

(2) Элементы конечного порядка в $\Bbbk^*$ – корни из 1.

Задача. Найдите способ вычислять порядки элементов в S_n. *Указание.* Разложить в произведение независимых циклов.

Предложение. $|a| = n < \infty \Longrightarrow a^m = n/\text{НОД}(n, m)$.

Доказательство. Пусть $d := \text{НОД}(n, m)$, $n' = n/d$. Тогда $(a^m)^{n'} = a^{nm/d} = 1$, $(a^m)^k = 1 \Longrightarrow n \mid mk \Longrightarrow n' \mid k$. □

Следствие. $\langle a \rangle = \langle a^m \rangle \Longleftrightarrow \text{НОД}(n, m) = 1$.

Теорема. (1) *Подгруппа циклической группы – циклическая.*

(2) *Порядок подгруппы в конечной циклической группе делит порядок группы.*

(3) $m \mid n \Longrightarrow$ *в циклической группе порядка n существует подгруппа порядка m и эта подгруппа – единственная.*

Доказательство. (1) Пусть $G = \langle a \rangle_n$ и пусть $H \subset G$ – подгруппа. Возьмем $m := \min\{k \in \mathbb{N} \mid a^k \in H\}$. Пусть $b := a^m$ и пусть $c \in H$. Тогда $c = a^l$, $l = mq + r$, $a^l = a^{mq} \cdot a^r$, $a^r = a^m \cdot (a^m)^{-q} \in H \Longrightarrow r = 0$ и $c = a^l = a^{mq} = b^q$.

(2) Пусть $G = \langle a \rangle_n$ и пусть $H \subset G$ – подгруппа. Тогда $H = \langle a^m \rangle \Longrightarrow |H| = |a^m| = n/\text{НОД}(n, m)$.

(3) Пусть $G = \langle a \rangle_n$ и пусть $n = mq$. Тогда положим $H = \langle a^q \rangle$. Имеем $|H| = |a^q| = n/\text{НОД}(n, q) = m$. Единственность: как в (1) . □

Предложение. *Пусть G – группа и пусть $a, b \in G$ – такие, что $ab = ba$. Пусть $|a| = n$, $|b| = m$ и $\text{НОД}(n, m) = 1$. Тогда $|ab| = nm$.*

Доказательство. Имеем $(ab)^{nm} = 1$. С другой стороны, если $(ab)^k = 1$, то $a^k = b^{-k}$, $1 = a^{nk} = b^{-nk}$, $-nk \equiv 0 \mod m$, $m \mid k$. □

Лекция 21

Изоморфизм циклических групп одного порядка. Смежные классы. Теорема Лагранжа. Малая теорема Ферма. Нормальные подгруппы. Свойства. Примеры. Факторгруппа

Теорема. *Все циклические группы одного порядка изоморфны:*

(1) *Бесконечная циклическая группа* $\simeq \mathbb{Z}$.

(2) *Конечная циклическая группа* $\simeq \mathbb{Z}/n\mathbb{Z} \simeq \boldsymbol{\mu}_u$.

Доказательство. (1) Отображение $\varphi : \mathbb{Z} \to G$, $k \mapsto a^k$ является изоморфизмом.
(2) Отображение $\varphi : \mathbb{Z}/n\mathbb{Z} \to G$, $\bar{k} \mapsto a^k$ является изоморфизмом. □

Смежные классы и теорема Лагранжа

Определение. Для любых подмножеств A, $B \subset G$ группы G положим

$$AB := \{ab \mid a \in A,\, b \in B\}.$$

В частности, для подгруппы $H \subset G$ и элемента $a \in H$ подмножество

$$aH := \{ah \mid h \in H\}$$

называется *левым смежным классом*. Аналогично определяются правые смежные классы.

Множество всех смежных классов обозначается G/H. Мощность множества G/H обозначается $[G : H]$ и называется *индексом* подгруппы H.

Заметим, что запись смежного класса в виде gH не является единственной:

Лемма. $gH = g'H \iff \exists\ h \in H \quad g' = gh$.

Доказательство. Если $gH = g'H$, то $g' \in gH$ и тогда $g' = gh$ для некоторого $h \in H$. Обратно, если $g' = gh$ для некоторого $h \in H$, то $g'h' = ghh' \in gH$ и поэтому $g'H \subset gH$. Аналогично доказывается обратное включение. □

Теорема. *Пусть G – группа и пусть $H \subset G$ – любая подгруппа.*

(1) *Группа G является объединением левых смежных классов $gH \in G/H$.*

(2) *Если два левых смежных класса g_1H и g_2H пересекаются, то они совпадают.*

(3) *Все левые смежные классы равномощны.*

Аналогичные утверждения верны для правых смежных классов.

Доказательство. (1) очевидно, поскольку $g \in gH$.

(2) Пусть $g \in g_1H \cap g_2H$. Тогда $g = g_1h_1 = g_2h_2$ для некоторых h_1, $h_2 \in H$. Отсюда $g_2 = g_1(h_1h_2^{-1})$ и $g_1H = g_2H$ по лемме.

(3) Отображение $H \to gH$, $h \mapsto gh$ является биекцией. □

Следствие (теорема Лагранжа)**.** *Если G – конечная группа, то*

$$|G| = |H|\ [G : H].$$

Следствие. *Порядок элемента делит порядок группы.*

Следствие. *Если $|G| = n$, то $a^n = 1 \quad \forall a \in G$.*

Следствие (Малая теорема Ферма)**.** *Пусть p – простое число. Тогда $m^p \equiv m \mod p$, $\forall m \in \mathbb{Z}$.*

Следствие. *Группа простого порядка – циклическая.*

Примеры. (1) $G = H \Longrightarrow G/H$ состоит из одного элемента.

(2) $G = S_n$, $H = A_n$. Имеется ровно 2 смежных класса: четные и нечетные подстановки.

Нормальные подгруппы

Определение. Подгруппа $H \subset G$ группы G называется *нормальной* (обозначается $H \lhd G$), если $gH = Hg \quad \forall g \in G$.

Примеры. (1) В абелевой группе любая подгруппа нормальна.

(2) В любой группе G имеются тривиальные нормальные подгруппы G и $\{1\}$.

(3) $SL_n(\Bbbk) \lhd GL_n(\Bbbk)$.

(4) $A_n \lhd S_n$.

Замечание. Подгруппа индекса 2 нормальна.

Замечание. Говорят, что элементы g и g' группы G сопряжены, если существует $x \in G$ такой, что $g' = xgx^{-1}$. (Не путайте с комплексным сопряжением!) Несложно проверить, что отношение сопряженности является отношением эквивалентности. Таким образом, группа G разбивается на непересекающееся объединение *классов сопряженных элементов*. Подгруппа H является нормальной тогда и только тогда, когда она составлена из классов сопряженных элементов.

Определение. *Центром* группы G называется подмножество

$$Z(G) := \{z \in G \mid gz = zg \quad \forall g \in G\}.$$

Очевидно, что центр – подгруппа и она нормальна (докажите самостоятельно). Более того, любая подгруппа $H \subset Z(G)$ нормальна в G.

Задача. Подгруппа $H \subset G$ порядка 2 нормальна тогда и только тогда, когда H содержится в центре. В частности, S_n не содержит нормальных подгрупп порядка 2.

Например, $Z(GL_n(\Bbbk))$ состоит из скалярных матриц, а $Z(SL_n(\Bbbk))$ состоит из скалярных матриц с определителем 1.

Предложение. *Следующие условия эквивалентны:*

(1) $H \lhd G$;

(2) $gHg^{-1} \subset H \quad \forall g \in G$.

Доказательство. Предположим, что $H \lhd G$, т.е. $gH = Hg \quad \forall g \in G$ и пусть $h \in H$. Тогда $gh \in Hg$. Следовательно, $gh = h'g$ для некоторого $h' \in H$ и поэтому $ghg^{-1} = h' \in H$. Это означает, что $gHg^{-1} \subset H$.

Предположим, что $gHg^{-1} \subset H$. Пусть $g \in G$ и пусть $gh \in gH$, где $h \in H$. Тогда $ghg^{-1} = h' \in H$. Следовательно, $gh = h'g \in Hg$ и поэтому $gH \subset Hg$. Обратное включение доказывается аналогично. □

Замечание. На самом деле, в условиях выше верно равенство $gHg^{-1} = H$. (Докажите самостоятельно).

Факторгруппы

Пусть H – нормальная подгруппа группы G (в мультипликативной записи). Напомним, что через G/H мы обозначаем множество всех левых смежных классов. Определим умножение смежных классов следующим образом:

$$(aH) \cdot (bH) = (ab)H.$$

Лемма. *Определенное выше умножение не зависит от способа записи смежных классов.*

Доказательство. Пусть $aH = a'H$ и $bH = b'H$. Тогда $a' = ah_1$ и $b' = bh_2$ для некоторых $h_1, h_2 \in H$. Имеем

$$a'b' = (ah_1)(bh_2) = (ab)(b^{-1}h_1b)h_2,$$

где $b^{-1}h_1b \in H$ (поскольку $H \lhd G$). Следовательно, $a'b' = abh$ для $h := (b^{-1}h_1b)h_2 \in H$ и поэтому $(aH) \cdot (bH) = (ab)H$. □

Предложение. *G/H является группой относительно определенного выше умножения.*

Доказательство. По определению имеем

$$(aH \cdot bH) \cdot cH = (ab)cH = a(bc)H = aH \cdot (bH \cdot cH).$$

Это доказывает ассоциативность операции. Нейтральным элементом в G/H является тривиальный смежный класс $1H = H$, а обратным к элементу aH является элемент $a^{-1}H$. □

Лекция 22

Теорема о гомоморфизме групп. Идеалы. Примеры. Факторкольца. Теорема о гомоморфизме колец. Присоединение к полю корня неприводимого многочлена.

Замечание. Отображение $\pi : G \to G/H$, $a \mapsto aH$ является гомоморфизмом групп.

Пример. Пусть $G := \mathbb{C}^*$ и пусть $H := \{z \mid |z| = 1\}$. Каждый элемент $z \in \mathbb{C}^*$ единственным образом записывается в виде $z = \alpha z_0$, где $\alpha \in \mathbb{R}_{>0}$, $z_0 \in H$. Поэтому каждый смежный класс G/H можно однозначно записать в виде αH, $\alpha \in \mathbb{R}_{>0}$. Следовательно, $G/H \simeq \mathbb{R}_{>0}$.

Теорема о гомоморфизме групп

Замечание. Пусть группа G порождается элементами $a_1, \ldots, a_n$. Если для двух гомоморфизмов $\varphi_1 : G \to G_1$ и $\varphi_2 : G \to G_1$ имеем $\varphi_1(a_i) = \varphi_2(a_i)$ для всех i, то $\varphi_1 = \varphi_2$.

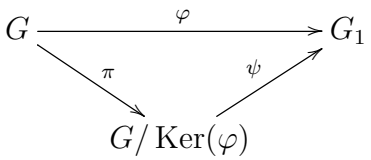
Теорема. *Пусть $\varphi : G \to G_1$ – гомоморфизм групп. Тогда*

(1) $\operatorname{Ker}(\varphi) \lhd G$.

(2) *Имеется естественный изоморфизм*

$$\psi : G/\operatorname{Ker}(\varphi) \to \varphi(G)$$

такой, что $\varphi = \psi \circ \pi$, где $\pi : G \to G/\operatorname{Ker}(\varphi)$ – естественный гомоморфизм на факторгруппу. В этом случае говорят, что диаграмма



коммутативна.

Доказательство. Положим $H := \operatorname{Ker}(\varphi)$. Для любого $b \in G$ имеем

$$a \in H \implies \varphi(a) = 1 \implies \varphi(bab^{-1}) = 1 \implies bab^{-1} \in H.$$

Следовательно, H – нормальная подгруппа.

Определим ψ следующим образом: $\psi(aH) = \varphi(a)$. Во-первых проверяем, что это определение корректно. Пусть $aH = a'H$. Тогда $a' = ah$ для некоторого $h \in H$. Отсюда

$$\psi(a'H) = \varphi(ah) = \varphi(a)\varphi(h) = \varphi(a) = \psi(aH).$$

Далее проверяем, что ψ – гомоморфизм:

$$\psi(aH \cdot bH) = \psi((ab)H) = \varphi(ab) = \varphi(a)\varphi(b) = \psi(aH)\psi(bH).$$

Далее

$$\psi(aH) = 1 \iff \varphi(a) = 1 \iff a \in H \iff aH = H.$$

Следовательно, ψ инъективно. Наконец, ψ сюръективно по построению. □

Примеры. (1) $S_n/A_n \simeq \{\pm 1\}$;

(2) $GL_n(\Bbbk)/SL_n(\Bbbk) \simeq \Bbbk^*$;

(3) $\mathbb{R}^*/\{\pm 1\} \simeq \mathbb{R}_{>0}$;

(4) $\mathbb{C}^*/\boldsymbol{\mu}_n \simeq \mathbb{C}^*$.

Идеалы

Определение. Подгруппа $I \subset R$ аддитивной группы кольца называется (двусторонним) *идеалом*, если $aI \subset I$ и $Ia \subset I$ для любого $a \in R$.

Примеры. (1) В каждом кольце имеется идеал $(0) := \{0\}$, который называется *нулевым*. Все кольцо R – также идеал.

(2) Четные числа – идеал в кольце $\mathbb{Z}$.

(3) Пусть $R = C[a,b]$ – кольцо действительных непрерывных функций на отрезке. Функции, обращающиеся в нуль а некоторой точке образуют идеал

$$I_c := \{f \in C[a,b] \mid f(c) = 0\}.$$

(4) В кольце матриц $\mathrm{Mat}_n(\Bbbk)$ аддитивная подгруппа

$$I := \left\{ \begin{pmatrix} 0 & * & \cdots & * \\ \cdots & \cdots & \cdots & \cdots \\ 0 & * & \cdots & * \end{pmatrix} \right\}$$

(матриц с нулевым левым столбцом) идеалом не является. Однако она является *левым идеалом*: $\forall A \in I, \quad \forall B \in \mathrm{Mat}_n(\Bbbk) \quad BA \in I$.

Определение. Пусть R – коммутативное ассоциативное кольцо и пусть $a_1, \ldots, a_n \in R$. Множество

$$(a_1, \ldots, a_n) := \{a_1 b_1 + \cdots a_n b_n \mid b_i \in R\}$$

является идеалом в R. Он называется *идеалом, порожденным элементами* $a_1, \ldots, a_n$. Это наименьший идеал, содержащий $a_1, \ldots, a_n$. Идеал, порожденный одним элементом, т. е. идеал вида

$$(a) := \{ab \mid b \in R\}$$

называется *главным*. Говорят, что R – *кольцо главных идеалов*, если в нем каждый идеал является главным. Если R – кольцо с единицей, то $(1) = R$. Этот идеал называется *единичным*.

Пример. Пусть R – коммутативное ассоциативное кольцо с единицей. Если некоторый идеал I содержит обратимый элемент, то он является единичным: $a \in I \Longrightarrow 1 = aa^{-1} \in I \Longrightarrow I = (1) = R$. Любой идеал в поле является или нулевым или единичным.

Факторкольца

Определение. Пусть I – идеал кольца R. На факторгруппе R/I аддитивной группы определим умножение по правилу $(a + I)(b + I) = ab + I$. Несложно проверить, что это определение не зависит от вида записи смежных классов $a+I$ и $b+I$: если $a+I = a'+I$ и $b + I = b' + I$, то $a' = a + c$ и $b' = b + d$ для некоторых c, $d \in I$. Отсюда

$$a'b' - ab = ad + cb + cd \in I$$

и поэтому $a'b' + I = ab + I$. Кольцо R/I называется *факторкольцом*.

Замечание. Отображение $\pi : R \to R/I$, $a \mapsto a + I$ является гомоморфизмом колец.

Замечание. Легко видеть, что

- кольцо R ассоциативно $\Longrightarrow$ R/I ассоциативно,
- кольцо R коммутативно $\Longrightarrow$ R/I коммутативно,
- кольцо R имеет единицу 1 и $1 \notin I \Longrightarrow$ R/I имеет единицу.

Теорема о гомоморфизме колец

Теорема (теорема о гомоморфизме колец)**.** *Пусть* $\varphi : R \to R_1$ *– гомоморфизм колец. Тогда*

(1) $\operatorname{Ker}(\varphi)$ *– идеал в* R.

(2) *Имеется естественный изоморфизм*

$$\psi : R/\operatorname{Ker}(\varphi) \longrightarrow \varphi(R)$$

такой, что $\varphi = \psi \circ \pi$, *где* $\pi : G \to R/\operatorname{Ker}(\varphi)$ *– естественный гомоморфизм на факторкольцо.*

Доказательство. Положим $I := \mathrm{Ker}(\varphi)$. Воспользуемся теоремой о гомоморфизме групп. Из нее следует, что I – подгруппа аддитивной группы R и имеется естественный изоморфизм групп $\psi : R/I \to \varphi(R)$, $\psi(a+I) = \varphi(a)$. Остается доказать, что ψ – гомоморфизм колец:

$$\psi((a+I)(b+I)) = \psi(ab+I) = \varphi(ab) = \varphi(a)\varphi(b) = \psi(a+I)\psi(b+I).$$

□

Примеры.

- Рассмотрим гомоморфизм $\varphi : C[a,b] \to \mathbb{R}$, $f \mapsto f(c)$. Тогда $\mathrm{Ker}\,\varphi = I_C$ и $C[a,b]/I_c \simeq \mathbb{R}$.
- Рассмотрим гомоморфизм $\varphi : \mathbb{R}[t] \to \mathbb{C}$, $f \mapsto f(i)$. Тогда $\mathrm{Ker}\,\varphi = (t^2+1)$ и $\mathbb{R}[t]/(t^2+1) \simeq \mathbb{C}$.

Присоединение к полю корня неприводимого многочлена

Пусть $\mathbb{L}$ – поле и пусть $\Bbbk \subset \mathbb{L}$ – подполе. Для элемента $\theta \in \mathbb{L}$ через $\Bbbk(\theta)$ мы обозначим подполе в $\mathbb{L}$, порожденное $\Bbbk$ и θ. Это наименьшее подполе в $\mathbb{L}$, содержащее $\Bbbk$ и θ.

Теорема. *Пусть $\Bbbk$ – поле и пусть $f \in \Bbbk[t]$ – многочлен положительной степени.*

(1) *Следующие три условия эквивалентны:*

   (a) *многочлен f неприводим,*

   (b) *факторкольцо $\Bbbk[t]/(f)$ является полем,*

   (c) *факторкольцо $\Bbbk[t]/(f)$ не имеет делителей нуля.*

(2) *Пусть многочлен f неприводим. Если $\mathbb{L}/\Bbbk$ – расширение полей такое, что f имеет корень $\theta \in \mathbb{L}$, то существует изоморфизм*

$$\varphi : \Bbbk[t]/(f) \to \Bbbk(\theta), \quad t \mapsto \theta,$$

являющийся тождественным отображением на $\Bbbk$.

Доказательство. (1) Докажем (1)(a) $\Longrightarrow$ (1)(b). Пусть $\pi : \Bbbk[t] \to \Bbbk[t]/(f)$ – естественный гомоморфизм. Рассмотрим ненулевой элемент $\bar{g} = g + (f) \in \Bbbk[t]/(f)$. Таким образом, $\bar{g} = \pi(g)$, где $g \in \Bbbk[t]$ – многочлен такой, что $g \notin (f)$. Последнее означает, что f и g взаимно просты (поскольку f неприводим). По теореме о наибольшем общем делителе существуют многочлены u, $v \in \Bbbk[t]$ такие, что $1 = fu + gv$. Отсюда

$$1 = \pi(1) = \pi(f)\pi(u) + \pi(g)\pi(v) = \bar{g}\pi(v).$$

Следовательно, любой ненулевой элемент $\bar{g} \in \Bbbk[t]/(f)$ обратим и поэтому $\Bbbk[t]/(f)$ – поле.

Импликация (1)(b) $\Longrightarrow$ (1)(c) очевидна. Для доказательства (1)(c) $\Longrightarrow$ (1)(a) предположим, что $f = f_1 f_2$, где $f_i \notin (f)$. Тогда в $\Bbbk[t]/(f)$ имеем

$$\pi(f_1)\pi(f_2) = \pi(f_1 f_2) = \pi(f) = 0,$$

т.е. $\pi(f_1)$, $\pi(f_2)$ – делители нуля. Противоречие.

(2) Рассмотрим отображение

$$\psi : \Bbbk[t] \longrightarrow \mathbb{L}, \qquad h \longmapsto h(\theta).$$

Ясно, что ψ – гомоморфизм. Его ядро является главным идеалом: $\mathrm{Ker}(\psi) = (h)$. С другой стороны, $f \in \mathrm{Ker}(\psi)$ и f неприводим. Поэтому $\mathrm{Ker}(\psi) = (f)$. По теореме о гомоморфизме $\psi(\Bbbk[t]) \simeq \Bbbk[t]/(f)$. □

Замечание. Построенное выше расширение называется *присоединением к полю корня неприводимого многочлена*. Действительно, поле $\Bbbk$ естественно вкладывается в $\Bbbk[t]/(f)$ (как композиция $\Bbbk \hookrightarrow \Bbbk[t] \xrightarrow{\pi} \Bbbk[t]/(f)$), а согласно (2) образ $\theta := \pi(t)$ является корнем многочлена f.